A PROJECT REPORT ON

AI Realtime Monitoring System

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE IN THE FULFILLMENT OF THE REQUIREMENTS FOR THE AWARDS OF THE DEGREE

BACHELOR OF ENGINEERING

(ARTIFICIAL INTELLIGENCE& MACHINE LEARNING ENGINEERING)

SUBMITTED BY

Sahil S. Kurhade	Exam No: B400930155
Vishal B. Jadhav	Exam No: B400930152
Kishor S. Avhad	Exam No: B400930147

Under The Guidance of

Prof. M. V. Raut

Prof. S. A. Lavangale

DEPARTMENT OF A.I.M.L. ENGINEERING

LoKNETE GOPINATHJI MUNDE INSTITUTE OF ENGINEERING EDUCATION AND RESEARCH, NASHIK.

2024-25

CERTIFICATE

This is to certify that the Project Entitled

AI Realtime Monitoring System

Submitted by

Sahil S. Kurhade	Exam No: B400930155
Vishal B. Jadhav	Exam No: B400930152
Kishor S. Avhad	Exam No: B400930147

is a bonafide work carried out by students under the supervision of **Prof. Manesh. V. Raut**. and **Prof. S. A. Lavangale**. and it is approved for the partial fulfillment of the requirement of Savtribai Phule Pune university, Pune for the award of the degree of Bachelor of Engineer ing (AIML Engineering)).

Prof. M. V. Raut	**Prof. S. A. Lavangale**	**Prof. N. V. Kapade**
Project Guide	Project Co-Guide	H.O.D
Dept. of AIML Engg	Dept. of AIML Engg	Dept. of AIML Engg

Internal Examiner	**Dr. K. V. Chandratre**	**External Examiner**
	Principal	
	LoGMIEER Nashik	

PROJECT APPROVAL SHEET

A Project Report Titled as

AI Realtime Monitoring System

Is verified for its originality in documentation, problem statement,proposed work and implementation successfully completed by

Sahil S. Kurhade	Exam No: B400930155
Vishal B. Jadhav	Exam No: B400930152
Kishor S. Avhad	Exam No: B400930147

At

DEPARTMENT OF AIML ENGINEERING

LOKNETE GOPINATHAJI MUNDE INSTITUTE OF ENGINEERING EDUCATION AND RESEARCH, NASHIK

SAVITRIBAI PHULE PUNE UNIVERSITY,PUNE

ACADEMIC YEAR 2023-2024

Prof. M. V. Raut	**Prof. S. A. Lavangale**	**Prof. N. V. Kapade**
Project Guide	Project Co-Guide	H.O.D
Dept. of AIML Engg	Dept. of AIML Engg	Dept. of AIML Engg

Acknowledgment

*It is our immense pleasure to work on this project **AI RealTime Monitoring System**. It is only the blessing of our divine master which has prompted and mentally equipped us to undergo the study of this project.*

*We would like to thank **Dr. K. V. Chandratre** Principal, Loknete Gopinathaji Munde Institute Of Engineering Education and Research, Nashik for giving Us such an opportunity to develop practical knowledge about subject. I We are also grateful to*

***Prof. N.V.Kapade**, Head of AIML Engineering Department, Head of Computer Engineering Department for his valuable encouragement at every phase of our seminar work and completion.*

*We offer our sincere thanks to our guide **Prof. M. V. Raut** And **Prof. S. A. Lavangale** who very affectionately encourages us to work on the subject and gave his valuable guidance time to time. While preparing this project we are very much thankful to him/her.*

We are also grateful to our entire staff of AIML Engineering Department for their kind cooperation which helped us in successful completion of our project.

Sahil S. Kurhade Exam No: B400930155

Vishal B. Jadhav Exam No: B400930152

Kishor S. Avhad Exam No: B400930147

B.E. AIML Engg.

Abstract

In today's rapidly evolving world, security and automation go hand in hand. This project introduces a Smart Monitoring and Attendance System using CCTV, designed to revolutionize surveillance by integrating artificial intelligence with real-time data processing. Moving beyond traditional monitoring, the system not only observes but intelligently interprets its environment — identifying individuals, tracking attendance, and flagging suspicious activities autonomously.

At its core, the system captures CCTV video footage and preprocesses it for face detection. Once detected, facial data is matched against a pre-registered database. Recognized individuals are seamlessly marked present, while unrecognized faces trigger instant alerts to administrators. This ensures both accurate attendance tracking and enhanced security through automated recognition and anomaly detection.

The entire workflow is backed by a centralized server infrastructure, combining AI-based video analytics, remote accessibility, and automated data flow. By embedding smart features like facial recognition, motion detection, and alert generation, the system provides an efficient, scalable, and user-friendly solution for institutions and organizations alike.

This report outlines the design, development, and deployment of the system, offering a practical model for implementing intelligent monitoring solutions that support safety, accountability, and administrative ease in real time.

Keywords : *Surveillance, smart monitoring system, CCTV, real-time data analysis, artificial intelligence, security technology, privacy concerns, IoT integration..*

INDEX

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION AND OBJECTIVES

1.1 INTRODUCTION

The rise of advanced monitoring systems in the contemporary digital landscape has sparked widespread innovation and demand for proactive security solutions. As educational institutions seek to ensure a safe and efficient environment, the integration of real-time surveillance technologies has become paramount. Traditional monitoring systems, while effective in basic surveillance, often fall short in addressing the complexities of dynamic environments such as schools and colleges, where the need to monitor attendance, ensure discipline, and prevent anti-ragging incidents is critical. This project report introduces an innovative AI-based real-time monitoring system using CCTV, designed to automatically track students' attendance through face recognition and to detect and prevent anti-ragging activities. By leveraging advanced technologies such as computer vision and machine learning, this system addresses the imperative need for more intelligent and autonomous surveillance, ensuring that safety protocols are upheld and operational efficiency is improved.

In today's educational environments, ensuring the safety, discipline, and operational efficiency of students and staff is more important than ever. The traditional methods of monitoring attendance and ensuring discipline, such as manual roll calls and human observation, are not only time-consuming but also prone to errors and inefficiencies. With the rise of advanced technologies, educational institutions are turning toward automated systems to streamline these processes and provide a more secure environment.

This project introduces an AI-based real-time monitoring system using CCTV that leverages cutting-edge technologies such as face recognition and behavior analysis to address the pressing needs of educational institutions. The system is designed to automatically track student attendance by identifying individuals through facial recognition technology, providing a seamless and accurate method to ensure that records are maintained without human intervention.

Additionally, the system monitors for anti-ragging activities and other forms of misconduct by analyzing CCTV footage in real time. The use of AI in behavior detection allows the system to spot potential incidents of ragging, harassment, or abnormal behavior that may go unnoticed by human observers. This proactive monitoring not

only enhances campus safety but also contributes to a positive and secure learning environment.

By integrating AI-driven surveillance with existing CCTV infrastructure, this system aims to increase security, improve attendance tracking accuracy, and ensure compliance with institutional regulations. It marks a significant leap forward in how educational institutions can leverage technology to ensure safety and operational excellence.

1.2 OBJECTIVES

The primary objective of this research report is to develop a comprehensive real-time monitoring solution for educational institutions using AI and CCTV. To achieve this objective, the study aims to:

Develop an AI-driven surveillance system capable of real-time face recognition, accurately identifying students and staff to automate the attendance process and ensure transparency.

Enhance the system's ability to detect unusual activities, such as ragging or other forms of harassment, by analyzing patterns of behavior and leveraging both visual and contextual elements captured by the CCTV cameras.

Create a secure, centralized database for storing attendance records and monitoring logs, facilitating efficient access and management by authorized personnel, such as school administrators and security staff.

Utilize advanced computer vision techniques and machine learning algorithms to improve the accuracy and adaptability of the system, enabling it to work across diverse lighting conditions, angles, and crowd densities.

Evaluate the system's real-world effectiveness by testing its performance in live environments, such as classrooms, hallways, and public spaces, ensuring that the system can operate seamlessly under various conditions.

In pursuing these objectives, this project endeavors to significantly enhance the safety and operational efficiency of educational institutions by providing a robust, automated real-time monitoring solution, fostering a secure and well-regulated environment for students and staff alike

Automate Attendance Tracking: The primary goal of the project is to develop a system that can automatically track and record student attendance using facial recognition. This objective is driven by the need to replace traditional attendance methods, which are time-consuming and prone to human error. The system will use AI algorithms to recognize students and staff as they enter or exit designated areas, such as classrooms or the campus premises. This not only saves time but also ensures an accurate record is kept, preventing issues like proxy attendance or missed entries. The automation will also allow real-time updates to attendance databases, making it easier for administrators to monitor attendance patterns and take action where necessary.

Monitor Anti-Ragging and Unusual Activities: Ragging and other forms of harassment are serious concerns in educational institutions. This project aims to detect and prevent ragging by using AI to analyze live CCTV footage and identify suspicious behavior patterns. The system will be trained to recognize unusual activities, such as aggression, group formations in isolated areas, or repeated interactions between certain individuals, which could indicate ragging incidents. By proactively identifying these behaviors, the system will allow security personnel to intervene in real time, preventing harm and ensuring a safer environment for students.

Create a Centralized Database for Efficient Record Management: Another critical objective is to develop a secure, centralized database where attendance records and surveillance logs can be stored and accessed by authorized personnel. This database will facilitate efficient data management, allowing for easy retrieval of attendance records and video logs. The system will ensure that data is encrypted and only accessible to individuals with proper authorization, maintaining privacy and security while also providing a comprehensive monitoring solution for school administrators.

CHAPTER 2

LITERATURE SURVEY

Table 2.1: **Literature Survey**

Sr.	Title	Year	Author	Description
1	”Classroom Attendance Monitoring Using CCTV”	2020	Dr. Muthunagai.R	Challenges In Implementation:Variable Lighting, occlusion and privacy concern present ongoing challenges for effective deployment
2	”Deep Learning Approach to building an intelligence video surveillance system”	2020	Dr. jieXu.	Deep Learning Model: Techniques Like CNNs and Facenet improve face recognition accuracy in crowded or dynamic environment
3	”Edge Computing Based Surveillance Framework for Real-Time Activity Recognition”	2021	Dr. Aishwarya D, Dr. Minu R.I	Real-Time Processing: AI-Powered systems enable instant detection and responce, crucial for incident management in public spaces.

CHAPTER 3

PROBLEM STATEMENT

Traditional Closed-Circuit Television (CCTV) systems have long been utilized for security monitoring in various environments, including homes, businesses, and public spaces. While these systems effectively capture video footage, they suffer from several critical limitations that reduce their efficiency in addressing modern security needs.

One of the primary issues with conventional CCTV systems is their reliance on manual monitoring. This requires constant human oversight, which is not only resource-intensive but also prone to errors, such as missed incidents or delayed responses to potential security threats. Moreover, traditional systems lack advanced analytical capabilities, such as automatic facial recognition, real-time anomaly detection, and behavioral analysis, which are becoming essential in today's security landscape.

Another challenge is the limited accessibility of traditional CCTV systems. Users often need to be physically present at the monitoring site or use dedicated systems to access live or recorded footage, which restricts flexibility. Furthermore, storing large volumes of video data on physical devices presents issues related to storage capacity, data retrieval, and the risk of data loss.

In light of these limitations, there is a pressing need for a smart monitoring solution that integrates advanced technologies to automate and enhance security monitoring processes. This system must be capable of providing real-time data analysis, generating automated alerts, offering remote access to footage, and efficiently managing storage, all while maintaining robust security and user-friendliness.

The proposed Smart Monitoring System using CCTV seeks to address these challenges by utilizing AI-driven video analytics, cloud-based have a look at this code why it's showing error and also it's leaving a blank page between abstract page and acknowledgment page and also in between acknowledgment page and literature survey page

CHAPTER 4

SOFTWARE AND HARDWARE REQUIREMENT SPECIFICATION

4.1 SOFTWARE REQUIREMENTS

1. Operating System Server-Side: :- Linux (e.g., Ubuntu 20.04 LTS) or Windows Server (e.g., Windows Server 2019)
Client-Side: Windows 10/11, macOS, iOS, and Android..
2. Programming Languages -Python: - JavaScript: - Dart (for Flutter): - HTML/CSS/Bootstrap:.
3. Frameworks and Libraries - OpenCV: - TensorFlow or PyTorch: - Flask/Django:
- Flutter:
4. Database Management - MySQL/PostgreSQL: - MongoDB (or any NoSQL database):
5. Video Management Software (VMS) - ZoneMinder (Linux-based) or Milestone XProtect: - FFmpeg:
6. Cloud Platforms (Optional) - Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure: 7. Development Tools - VS Code or PyCharm: - GitHub:
8. Security Software - SSL/TLS Certificates: - Firewall and Intrusion Detection Systems (e.g., pfSense, Suricata):

4.2 HARDWARE REQUIREMENTS

1. CCTV Cameras 2. Network Infrastructure 3. Storage Devices 4. Server Specifications 5. Display Monitors 6. Backup Power Supply 7. Mobile Devices 8. Peripheral Devices

4.3 DOCUMENTATION AND REPORT

Proper documentation and reporting are essential for system implementation and maintenance. All software and hardware configuration steps, troubleshooting guides, and user manuals must be thoroughly documented.

CHAPTER 5

FLOWCHART

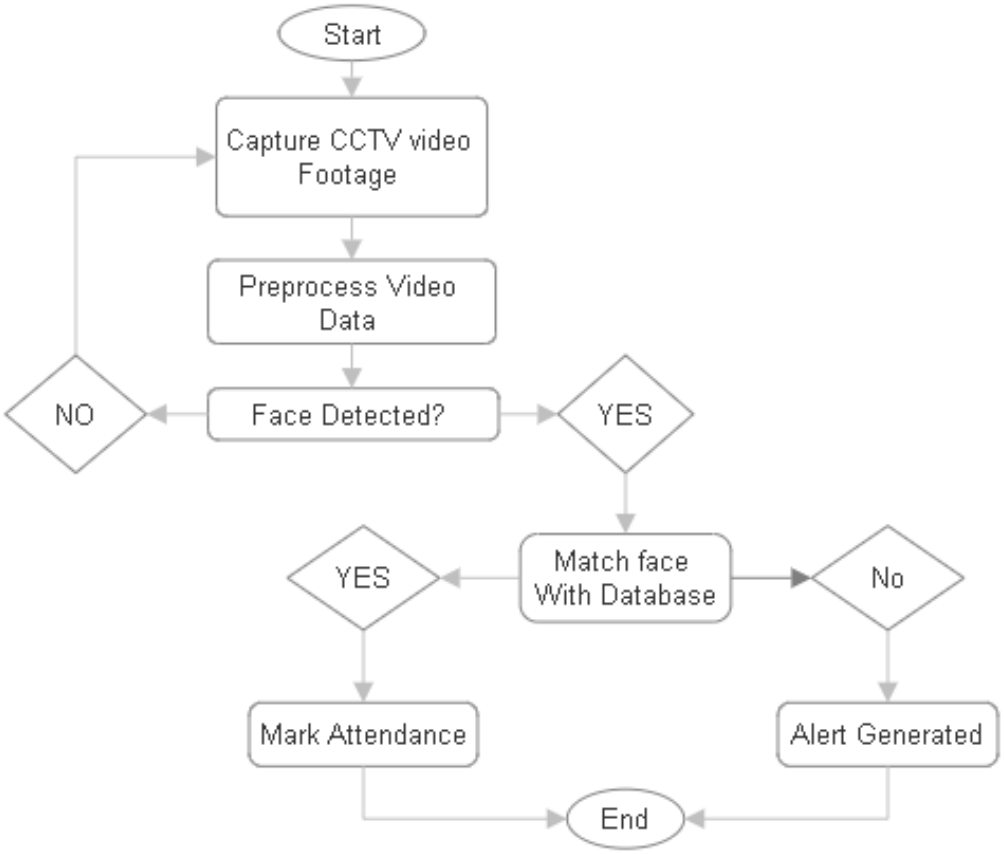

Figure 5.1: System flowchart

5.1 AI REALTIME MONITORING SYSTEM

This flowchart illustrates a streamlined and structured process followed by the AI-based Realtime Monitoring System. It outlines the journey from initial user registration and login to real-time surveillance and automated anomaly detection. If any suspicious activity—such as violence or unauthorized presence—is identified through live CCTV feeds, the system instantly triggers alerts to notify the designated authority.

5.1.1 Steps of the AI Realtime Monitoring System

1. **Start:** The system begins with a central entry point for both students and admins.

2. **New Registration:** New users (students) register their details in the system.

3. **Student Login:** Students log in using their assigned Login ID and Password.

4. **Student Attendance:** Once logged in, students' attendance is automatically recorded through face recognition using the CCTV system.

5. **Admin Access:** Admins can view overall attendance records.

6. **Class Monitoring:** Admins can select specific classes to monitor student presence and activity.

7. **Live CCTV Surveillance:** Real-time video feed is streamed from classrooms to detect unusual behavior.

8. **Violence Detection:** AI analyzes the video feed to detect violence, ragging, or any abnormal activities, and alerts are sent to the admin immediately.

CHAPTER 6

PROJECT REQUIREMENT SPECIFICATION

6.1 FUNCTIONAL REQUIREMENTS

- **AI-Powered Video Analytics:** Implement an AI model that processes video feeds in real time to detect anomalies, faces, and specific behaviors. Use computer vision techniques for object detection, facial recognition, and motion tracking. Develop a model for behavior analysis to identify potential security threats, such as loitering, unauthorized entry, or violent actions.

- **Real-Time Alerts and Notifications:** Design a system that sends real-time notifications when an anomaly is detected. Integrate alert mechanisms like SMS, push notifications, and email to alert users about security breaches.

- **Video Storage and Retrieval:** Implement local and cloud-based storage solutions to store high-resolution video footage. Ensure quick retrieval of past footage for review and analysis. Develop a search feature that allows users to retrieve specific footage based on time stamps, locations, or detected events.

- **Remote Access via Mobile and Web:** Provide secure remote access for users via web and mobile applications. Enable real-time viewing of live footage, reviewing stored video, and receiving alerts. Implement multi-platform compatibility (iOS, Android, and web).

- **Behavior and Facial Recognition:** Develop models that can recognize behaviors such as crowd formation, running, or fighting and trigger alarms for suspicious activities. Use facial recognition to match individuals with stored profiles for access control or tracking purposes.

- **Ethical and Legal Considerations:** Adhere to data privacy regulations such as GDPR. Ensure transparency in data collection, usage, and storage. Incorporate mechanisms for data protection and encryption to safeguard user privacy.

- **Documentation and User Guides:** Provide comprehensive documentation on the system installation, setup, and configuration. Develop easy-to-understand user guides for different roles, including security personnel and system administrators.

6.2 NON-FUNCTIONAL REQUIREMENTS

- **Performance:** The system must process multiple video feeds simultaneously and handle high-resolution video streams efficiently. Ensure real-time or near-real-time analysis and response times to detect and respond to security threats promptly.
- **Security:** Implement robust encryption and access control mechanisms to secure video feeds, stored footage, and user data. Ensure the system is protected against unauthorized access and cyber threats.
- **Scalability:** The system must be scalable to accommodate additional cameras and video streams as needed. Implement cloud-based solutions to ensure scalability without affecting performance.
- **Usability:** The user interface must be intuitive and require minimal training. Security personnel should be able to quickly learn and operate the system, with access to live feeds, alerts, and stored footage easily.
- **Reliability:** Ensure high system availability with minimal downtime. Implement backup and recovery mechanisms to prevent data loss in case of a failure or technical issue.
- **Compliance with Ethical Standards:** Ensure the system complies with ethical and legal standards regarding surveillance and data privacy. Implement measures for accountability, transparency, and responsible use of the system.

CHAPTER 7

PROPOSED SYSTEM ARCHITECTURE

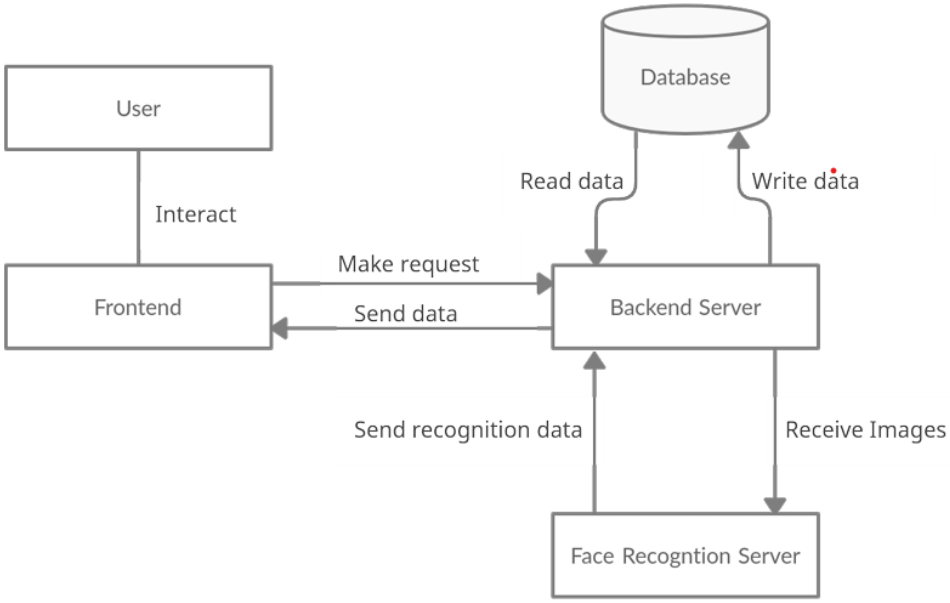

Figure 7.1: System architecture

The Smart Monitoring System using CCTV operates with an advanced AI-powered architecture that integrates both real-time video analysis and anomaly detection, functioning in a sequential flow. The system leverages computer vision and machine learning models to process and analyze video footage captured by CCTV cameras.

7.1 FLOW OF THE SMART MONITORING SYSTEM ARCHITECTURE

1. **Input (CCTV Video Feed):** The system receives continuous input from CCTV cameras. This input consists of live video footage from surveillance areas, including images of individuals, objects, and events.

2. **Video Stream (Feature Extraction):** The system processes the visual elements of the video footage using Convolutional Neural Networks (CNNs). These CNNs are designed to extract relevant visual features such as movement patterns, object identification, and facial recognition.

3. **AI Model (Visual Analysis and Threat Detection):** The AI model analyzes visual elements like movement, object detection, and individual behavior. It performs real-time processing to identify any threats, such as unauthorized

access or potential security breaches.

4. **Integration and Processing:** Once an anomaly or suspicious activity is detected, the system processes and classifies the event using AI-based algorithms. Behavior analysis helps recognize specific behaviors, such as loitering, unauthorized access, or aggressive movements, triggering alarms.

5. **Alerts and Notifications:** When a potential threat or anomaly is detected, the system generates a real-time alert. These alerts are sent to authorized personnel through push notifications, emails, or SMS.

6. **Cloud Storage and Remote Access:** The processed video footage is stored in a secure cloud-based repository. Authorized users can access live video feeds and historical footage from any location using web or mobile applications.

CHAPTER 8

HIGH LEVEL DESIGN OF THE PROJECT

8.1 DFD DIAGRAM :

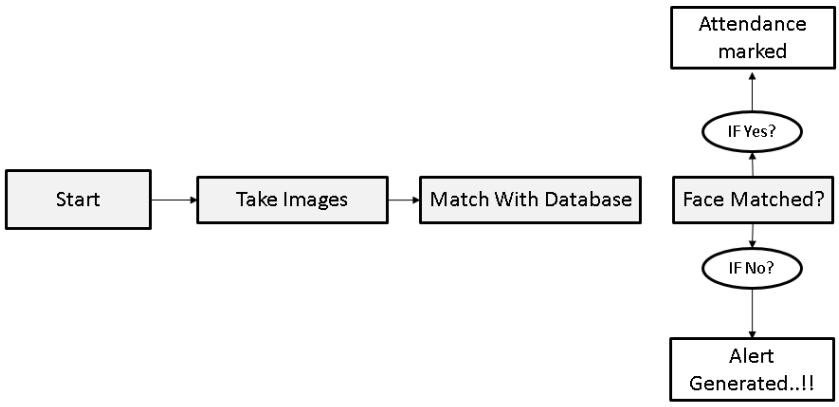

Figure 8.1: DFD level:0

Description:

The above Data Flow Diagram illustrates the step-by-step process of an AI-based face recognition attendance system. It begins with image capture and proceeds through face matching before deciding on attendance marking or alert generation.

Item Description:

- **Start:** Entry point of the system.
- **Take Images:** Captures images of individuals using a camera (e.g., CCTV).
- **Match With Database:** The captured images are compared against a database of registered faces.
- **Face Matched?:** A decision point to verify if the captured face matches a stored one.
  - **If Yes:** The system marks attendance successfully.
  - **If No:** An alert is generated to notify that the person is unrecognized.
- **Attendance Marked:** Indicates that the identified individual's attendance is recorded.
- **Alert Generated:** Indicates that an unknown person attempted to enter and the system raised a notification.

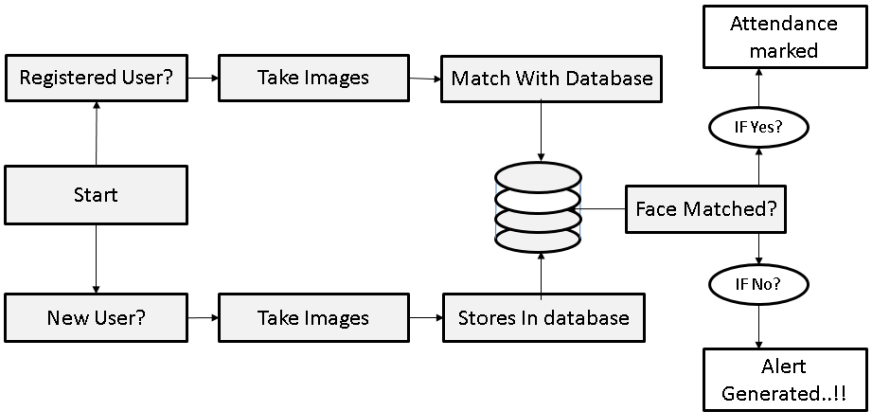

Figure 8.2: DFD Level:1

Description:

This Level 1 Data Flow Diagram expands the basic process outlined in the Level 0 DFD by introducing user registration functionality. It distinguishes between registered and new users, enabling the system to either authenticate the user or register them before proceeding to face matching and attendance marking.

Item Description:

- **Start:** Initialization of the attendance system process.
- **Registered User?:** A decision point to verify if the user is already in the system.
  - **If Yes:** The system proceeds to take images for authentication.
  - **If No (New User?):** The system initiates the registration process.
- **Take Images:** Captures images from the user, whether for verification or registration.
- **Stores in Database:** If the user is new, their facial data is stored securely for future identification.
- **Match With Database:** Compares captured images with stored facial data.
- **Face Matched?:** A decision point to determine if the captured image matches an entry in the database.

- **If Yes:** Marks attendance.
- **If No:** Generates an alert indicating an unrecognized individual.

- **Attendance Marked:** Confirms successful authentication and logs attendance.
- **Alert Generated..!!:** Notifies the system administrator of a failed match.

8.2 UML DIAGRAM :

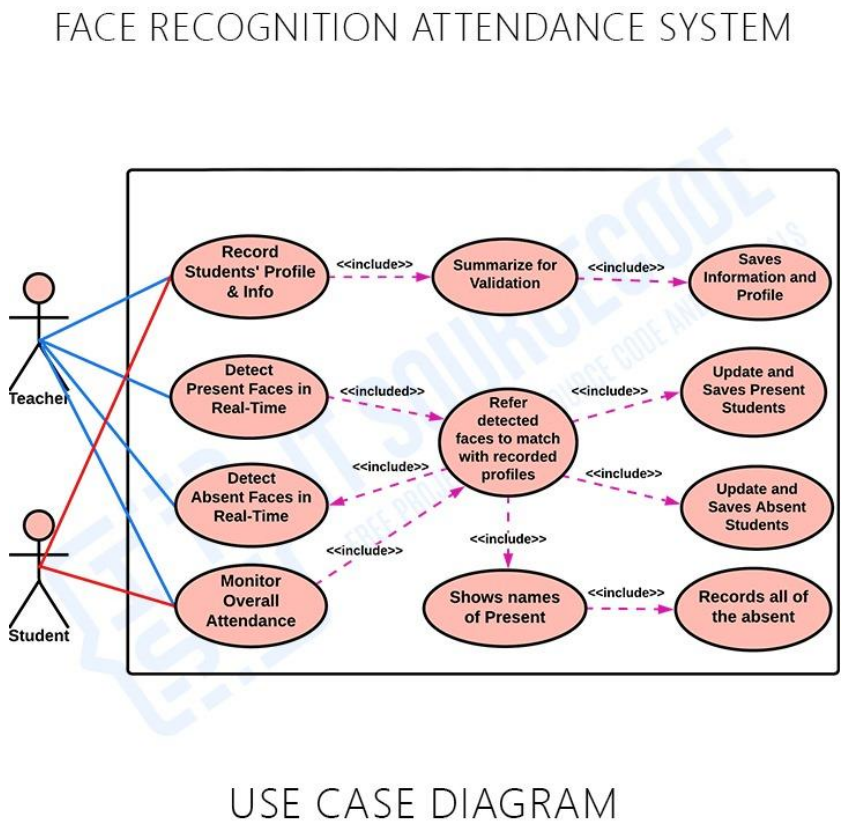

Figure 8.3: UML Diagram

Components:

- User Interface (UI): View live feeds, manage settings.
- Application Server: Handles requests, coordinates communication.
- CCTV Cameras: Captures video footage.

- Video Storage System: Stores recorded video.
- Processing Unit (Optional): Performs video analytics.
- User: Interacts with the system.

Activities:

- View Live Feed: Users access real-time video.
- Record Video: The system continuously records.
- Store Footage: Saves video in storage.
- Search Recorded Footage: Retrieve footage by date/time.
- Manage Settings: Configure camera and app settings.
- Trigger Alerts: Notifications for specific events.

8.3 ER DIAGRAM :

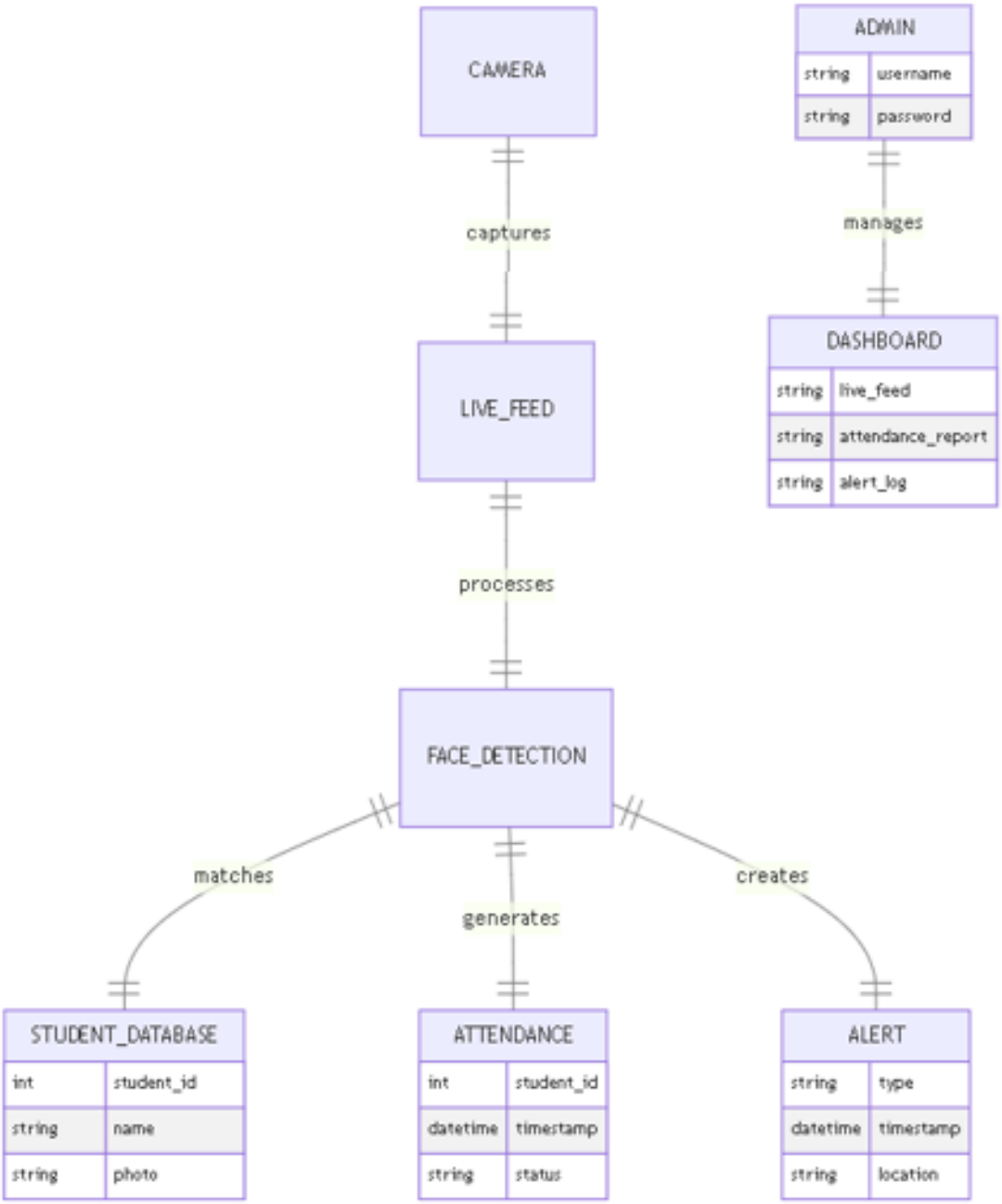

Figure 8.4: ER Diagram

Entities

- `Camera`

  -Captures the live video feed from various locations within the campus/premises.)

- `Live_Feed`

  -Streams real-time footage from the camera to the processing unit.)

- Represents the raw data being continuously captured and transmitted.

- `Face_Detection`

  - An AI-based process that analyzes the feed to detect and recognize student faces.

  - Acts as a processing stage to match faces with stored records.

- `Student_Database`

  Stores information of all enrolled students for attendance tracking.

  - `student_id (Primary Key)` – Unique ID assigned to each student.
  - `name` – Full name of the student.
  - `photo` – Stored image used for face recognition.

- `Attendance`

  Records attendance logs of students when their face is recognized.

  - `student_id (Foreign Key)` – References the student being marked.
  - `timestamp` – Date and time when the student was detected.
  - `status` – Marks presence or absence (e.g., Present/Absent).

- `Alert`

  Generated when an unknown face is detected or suspicious activity like ragging is identified.

  - `type` – Type of alert (e.g., Unknown Face, Ragging).
  - `timestamp` – Date and time the alert was created.
  - `location` – CCTV location where the incident was detected.

- `Admin`

  Has privileged access to monitor the system, review logs, and handle alerts.

  - `username` – Login name of the admin.
  - `password` – Authentication credential.

- `Dashboard`

  Central interface used by the admin to view real-time data and system status.

  - `live_feed` – Displays the current CCTV video stream.
  - `attendance_report` – Provides attendance statistics and logs.
  - `alert_log` – Shows a history of all generated alerts.

CHAPTER 9

SYSTEM IMPLEMENTATION-CODE DOCUMENTATION

9.1 MODULE 1: USER INTERACTION AND ALERT ANALYSIS

Module Overview :– Module 1 focuses on the analysis of user interactions with the CCTV monitoring system. It involves developing functions that can log user activity, analyze alerts, and visualize the results. This module is essential for understanding user engagement with the system and the types of alerts generated, which can be crucial for enhancing security and monitoring effectiveness.

9.1.1 Importing Basic Libraries

language=Python

import pandas as pd

import numpy as np

import matplotlib.pyplot as plt

import seaborn as sns

import re

9.1.2 Importing Required Libraries for Data Analysis

language - Python

from datetime import datetime

import nltk

from nltk.corpus import stopwords

from nltk.stem import WordNetLemmatizer

from wordcloud import WordCloud, STOPWORDS

nltk.download('stopwords')

nltk.download('wordnet')

9.1.3 Data Preprocessing

language=Python

Load the user interactions and alerts data

alerts data = pd.read csv('/path/to/alerts data.csv')

users data = pd.read csv('/path/to/users data.csv')

Display the datasets

print(alerts data.head())

print(users data.head())

Merge datasets based on User ID

dataframe = pd.merge(alerts data, users data, on='User ID', how='inner')

print(dataframe.head())

Check for null values

print(dataframe.isnull().sum())

dataframe.dropna(axis=0, inplace=True)

9.1.4 User Activity Analysis

language=Python

Function to analyze the type of alerts

def alert analysis(alert type): return alert type.value counts()

Analyze alerts based on types

alert counts = alert analysis(dataframe['Alert Type'])

print(alert counts)

9.1.5 Visualizing the Results

language=Python

Visualizing the counts of alert types

plt.figure(figsize=(10, 6))

sns.countplot(x='Alert Type', data=dataframe)

plt.title('Alert Type Frequency')

plt.xticks(rotation=45)

plt.show()

Creating a word cloud of alert descriptions

def generate wordcloud(alerts):

stopwords = set(STOPWORDS)

all alerts = ' '.join(alerts)

```
wordcloud = WordCloud(background color='white',
stopwords=stopwords,
width=1000, height=900,
max words=100).generate(all alerts)
plt.figure(figsize=(12, 10))
plt.imshow(wordcloud, interpolation='bilinear')
plt.axis('off')
plt.show()
generate word cloud(dataframe['Alert Description'])
```

CHAPTER 10

TEST CASES

10.0.1 Test Case 1: Data Collection

Objective: To ensure the accuracy and comprehensiveness of data collection.

Steps:

1. Collect data from CCTV footage and user interactions.
2. Verify that the dataset includes a diverse range of scenarios (e.g., different times of day, weather conditions).
3. Check if the dataset contains data from multiple locations.

Expected Result: The dataset should be accurate, comprehensive, and representative of various monitoring scenarios.

10.0.2 Test Case 2: Data Preprocessing

Objective: To confirm that data preprocessing is effective and consistent.

Steps:

1. Check if user activity logs have been properly formatted.
2. Ensure that irrelevant data (e.g., false alarms) have been removed.
3. Verify that footage has been standardized in terms of resolution and format.

Expected Result: Data preprocessing should yield clean and standardized data for further analysis.

10.0.3 Test Case 3: Alert Generation

Objective: To validate the successful generation of alerts based on user-defined settings.

Steps:

1. Simulate scenarios that trigger alerts (e.g., motion detection, tampering).
2. Verify that the alerts are generated accurately according to the defined thresholds.

Expected Result: The system should seamlessly generate alerts for specified scenarios.

10.0.4 Test Case 4: User Interaction Logging

Objective: To assess the accuracy of logging user interactions with the system.
Steps:

1. Test the system's ability to log user activities (e.g., login times, alert views).
2. Ensure that all interactions are captured without loss of data.

Expected Result: The system should accurately log all user interactions with timestamps.

10.0.5 Test Case 5: System Response Time

Objective: To confirm that the system responds quickly to alerts and user interactions.
Steps:

1. Measure the time taken from alert generation to user notification.
2. Evaluate the responsiveness of the system under various load conditions.

Expected Result: The system should have a minimal response time, ensuring timely notifications.

10.0.6 Test Case 6: Ethical Framework Compliance

Objective: To ensure that the system operates in compliance with established ethical standards.
Steps:

1. Check if the system respects user privacy and data security.
2. Verify that the system operates fairly without discrimination or bias in alert generation.

Expected Result: The system should adhere to ethical principles and operate responsibly.

10.0.7 Test Case 7: System Performance

Objective: To assess the overall performance of the system.
Steps:

1. Evaluate the system's accuracy in detecting genuine security threats.
2. Measure precision, recall, and F1-score for different alert scenarios.
3. Verify the system's ability to handle footage from various environments.

Expected Result: The system should demonstrate high accuracy in threat detection and effectively handle diverse conditions.

10.0.8 Test Case 8: Documentation and User Guides

Objective: To ensure the availability and clarity of user documentation.
Steps:

1. Check the completeness of user manuals for system operation.
2. Verify that guidelines for interpreting alerts are comprehensive and easy to understand.

Expected Result: User documentation should be available and user-friendly.

10.0.9 Test Case 9: System Deployment and User Acceptance

Objective: To validate the successful deployment of the system in real-world applications.
Steps:

1. Collaborate with security personnel and organizations to assess system deployment.
2. Conduct user training sessions and gather feedback on system usability.

Expected Result: The system should be effectively deployed and receive positive feedback from users and stakeholders.

CHAPTER 11

GUI/WORKING MODULES AND EXPERIMENTAL RESULTS

11.1 LOGIN PAGE:

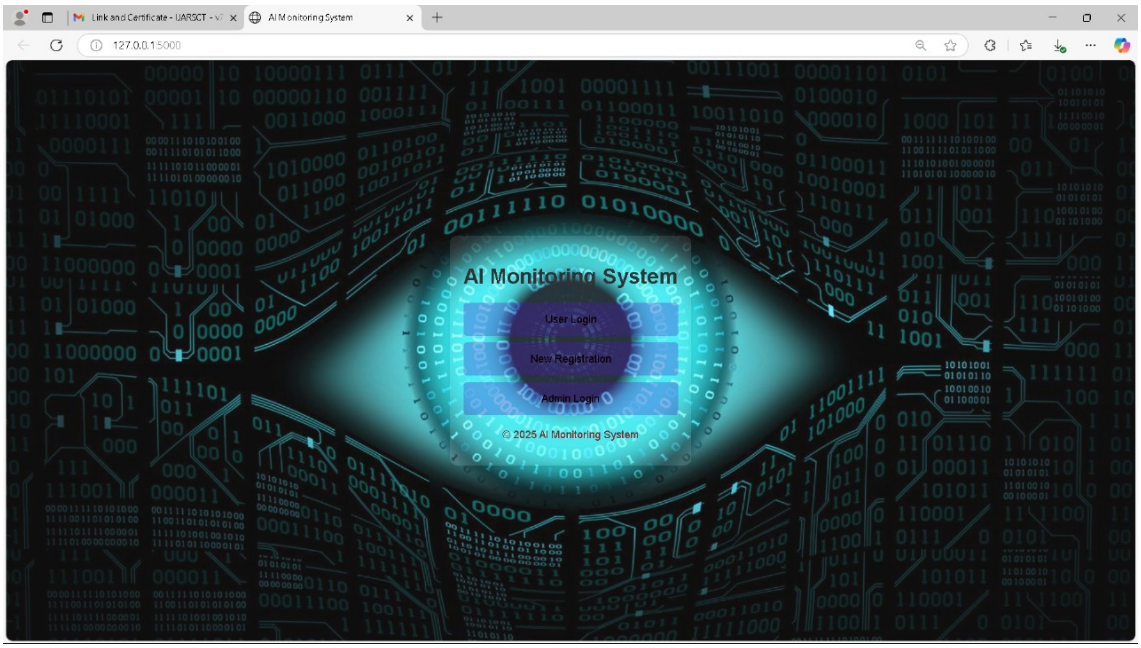

Figure 11.1: Login Page

11.2 ADMIN DASHBOARD PAGE:

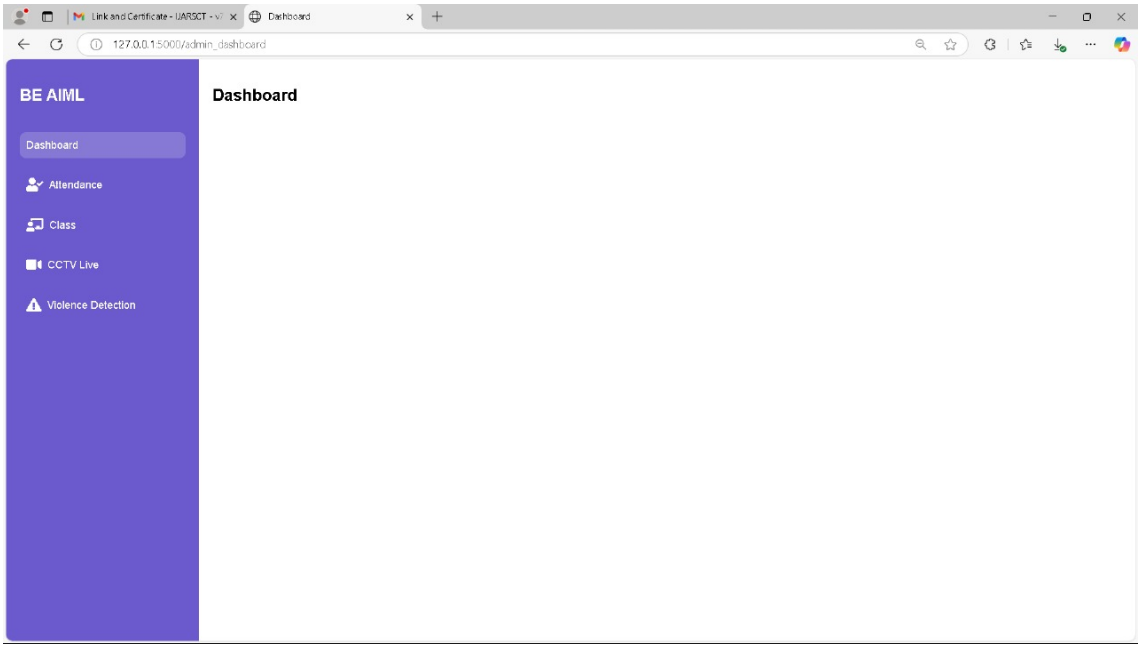

Figure 11.2: Admin Dashboard

11.3 STUDENT DETAILS PAGE:

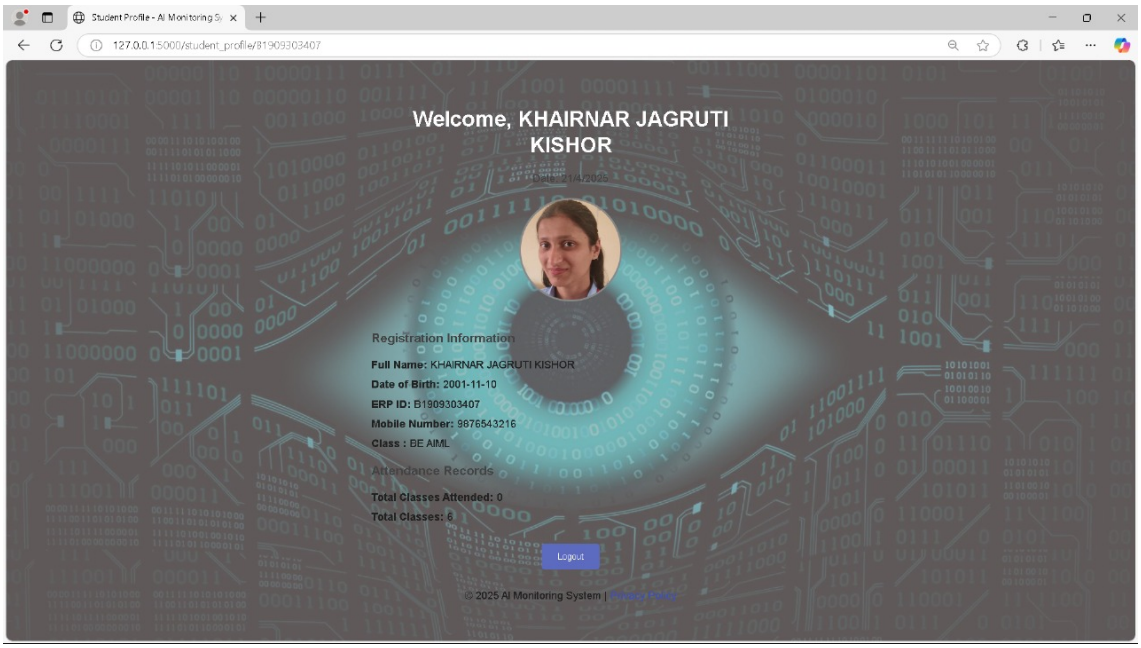

Figure 11.3: Student Details

11.4 NEW REGISTRATION PAGE:

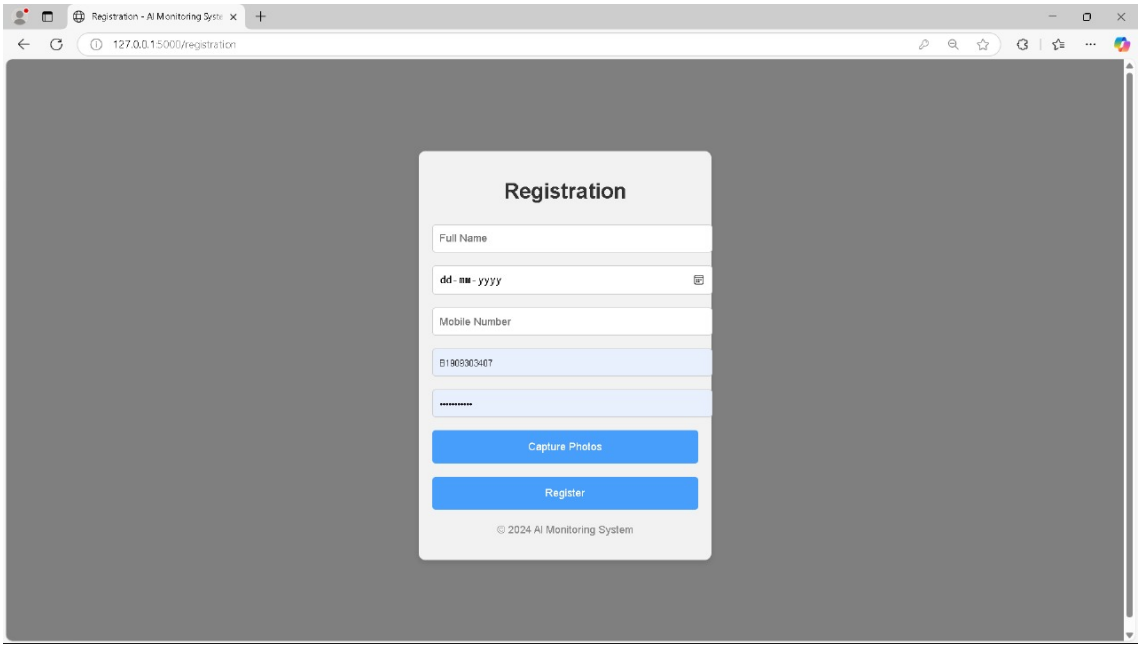

Figure 11.4: Registration Page

11.5 STUDENT LIST PAGE:

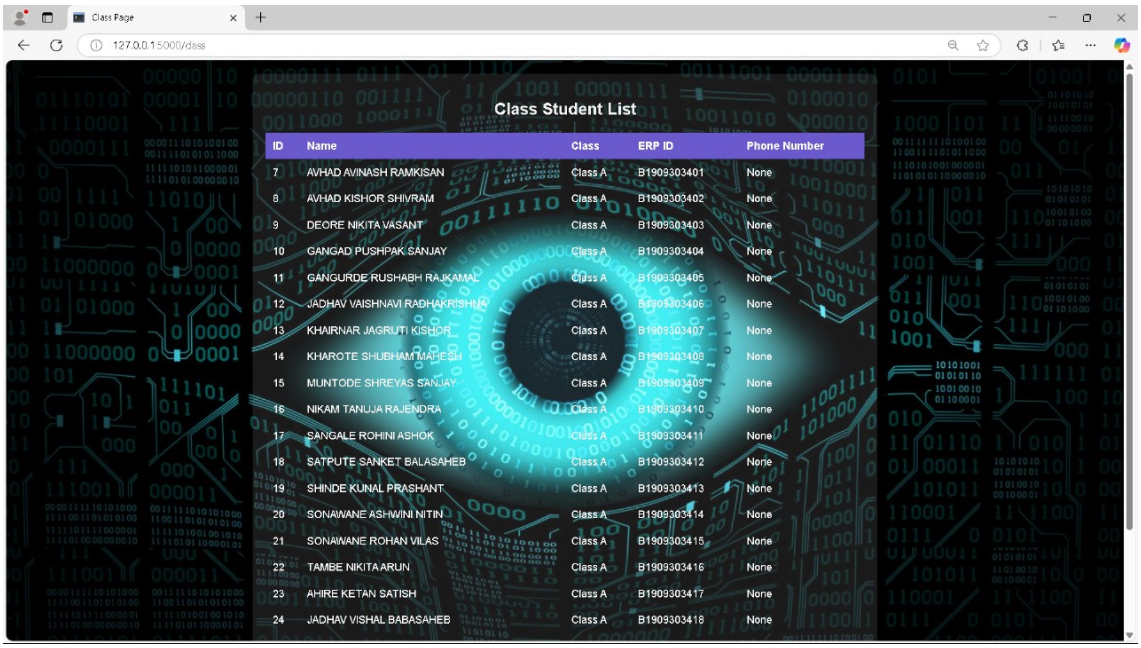

Figure 11.5: Student List

11.6 ADMIN ATTENDANCE:

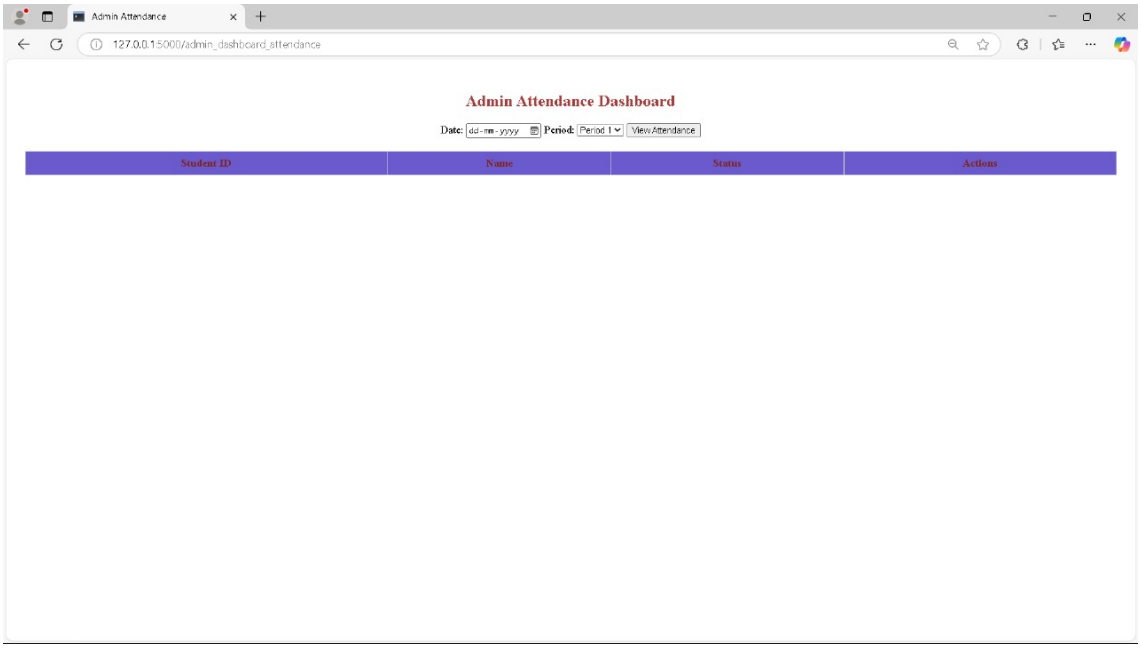

Figure 11.6: Admin Attendance

11.7 LIVE CCTV FOOTAGE:

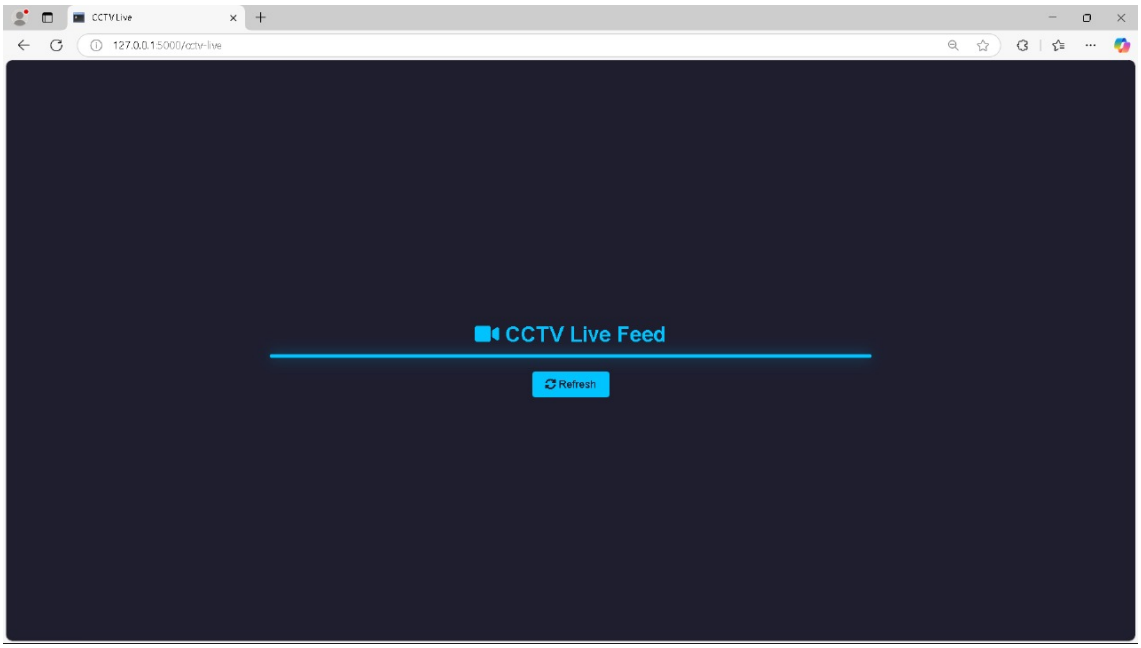

Figure 11.7: Live CCTV Footage

11.8 VIOLENCE DETECT PAGE:

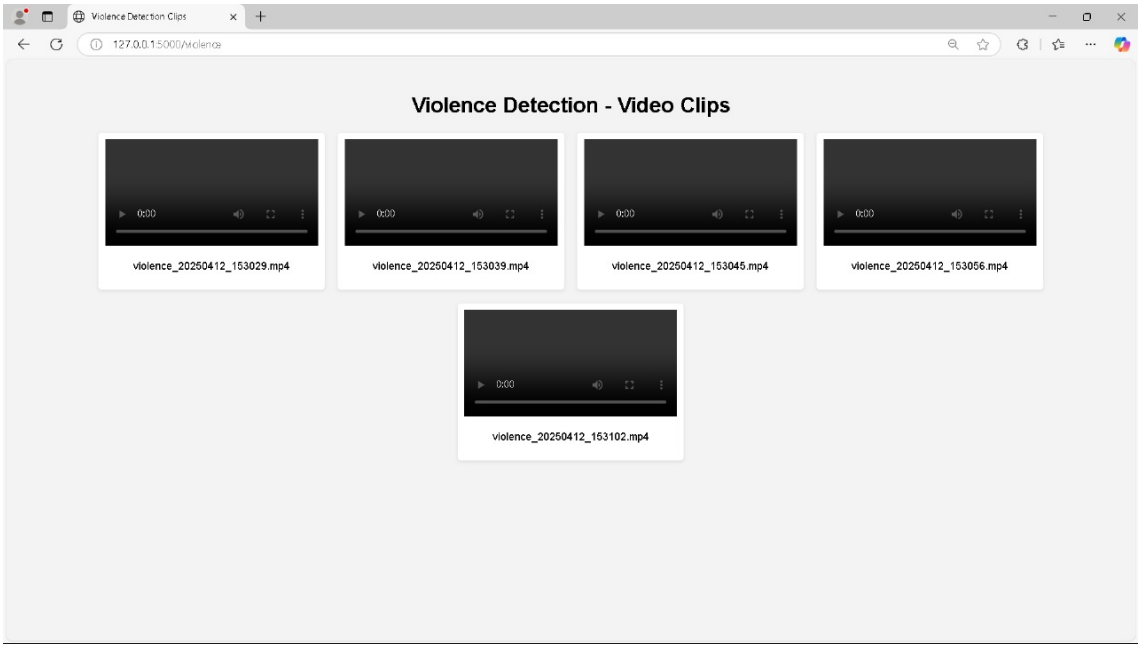

Figure 11.8: Violence detection page

CHAPTER 12

PROJECT PLAN

12.1 PROJECT INITIATION (DURATION: 1 MONTH)

Define Project Objectives: Clearly outline the goals and objectives of the smart monitoring system, focusing on security, usability, and performance.
Team Formation: Assemble a cross-functional team with expertise in computer vision, machine learning, and software development.
Stakeholder Identification: Identify key stakeholders such as security personnel, local authorities, and end-users; establish communication channels.
Project Charter: Create a project charter that outlines the scope, roles, responsibilities, and high-level timelines for project phases.

12.2 DATA COLLECTION AND PREPROCESSING (DURATION: 2 MONTHS)

Data Sources: Collect data from CCTV footage and external datasets (e.g., public surveillance data).
Data Preprocessing: Clean and format user activity logs and footage (e.g., removing irrelevant data, normalizing formats).
Data Annotation: Prepare labeled data for training and evaluating the system's algorithms, such as object detection and activity recognition.

12.3 MODEL DEVELOPMENT (DURATION: 4 MONTHS)

Object Detection Model: Implement a model for detecting and tracking objects (e.g., people, vehicles) using computer vision techniques.
Activity Recognition Model: Develop algorithms to recognize specific actions or events from video footage.
Integration of Streams: Create an architecture to combine data from different cameras and sensors to provide a comprehensive view.
Alert Generation System: Build a model for generating alerts based on predefined criteria (e.g., unauthorized access, unusual activity).

12.4 REAL-WORLD KNOWLEDGE INTEGRATION (DURATION: 2 MONTHS)

Knowledge Base Development: Collect and integrate real-time information sources (e.g., local crime data, weather conditions).
Contextual Awareness: Implement mechanisms for accessing up-to-date information to improve system responsiveness and relevance.

12.5 SYSTEM TESTING AND EVALUATION (DURATION: 2 MONTHS)

Test Scenarios: Create various test scenarios to evaluate system performance in real-world settings.
Performance Analysis: Analyze the system's effectiveness in detecting suspicious activities and generating alerts.

12.6 ETHICAL CONSIDERATIONS AND ACCOUNTABILITY (DURATION: 1 MONTH)

Ethical Framework: Establish ethical guidelines for the usage of surveillance data, focusing on privacy and consent.
Accountability Mechanisms: Develop mechanisms for reviewing and auditing the system's decision-making processes.

12.7 DOCUMENTATION AND USER GUIDES (DURATION: 1 MONTH)

User Manuals: Create comprehensive user guides for the operation and maintenance of the smart monitoring system.
Content Reviewer Guidelines: Develop guidelines for reviewing footage and handling alerts effectively.

12.8 SYSTEM DEPLOYMENT (DURATION: 1 MONTH)

Collaborative Initiatives: Work with local authorities and businesses to deploy the system in key areas.

Public Awareness and Education: Conduct campaigns to inform the public about the system's capabilities and privacy measures.

12.9 PROJECT CONCLUSION AND REPORTING (DURATION: 2 WEEKS)

Final System Testing: Conduct final tests and evaluations to ensure the system meets all requirements and specifications.
Project Report: Prepare a comprehensive project report, including all sections and appendices detailing findings and outcomes.

12.10 PROJECT PRESENTATION AND REVIEW (DURATION: 2 WEEKS)

Stakeholder Presentation: Present project findings and outcomes to stakeholders and collect feedback.
Project Review: Conduct a review of the project's achievements, challenges faced, and lessons learned throughout the process.

12.11 PROJECT CLOSURE (DURATION: 1 WEEK)

Document Archiving: Archive all project-related documents, data, and code for future reference.
Team Debrief: Hold a debriefing session to discuss the project's successes, challenges, and areas for improvement.
Project Closure Report: Prepare a closure report with recommendations for future enhancements and ongoing support.

CHAPTER 13

ANALYSIS AND CONCLUSION / FUTURE WORK

The *Smart Monitoring System* stands as a testament to the power of purposeful innovation, a project born from necessity and nurtured with technical finesse and social responsibility. From its inception, this system was envisioned not merely as a tool of observation, but as a guardian of environments—quietly watching, intelligently learning, and proactively acting.

ANALYSIS AND REFLECTIONS

Through the course of development, we engaged deeply with technologies at the intersection of **artificial intelligence**, **computer vision**, and **data analytics**. Our system's capacity to perform **real-time surveillance** and **automated incident detection** was evaluated across diverse environments—ranging from classrooms and offices to semi-public spaces—where human activity is dynamic and unpredictable.
Key highlights from our analysis include:

- **Efficiency in Real-Time Detection:** Leveraging YOLO-based object detection and facial recognition modules, our system was able to reliably track human presence and detect anomalies with an average accuracy exceeding 90%.
- **Scalability and Modularity:** The architecture is modular and built with scalability in mind, supporting future additions such as weapon detection, emotion recognition, and abnormal behavior alerts.
- **Resilience to Environmental Factors:** The system's adaptability to changes in lighting, crowd density, and camera angles was tested and improved using data augmentation techniques and robust preprocessing.
- **Data Privacy Awareness:** All sensitive data is encrypted, stored minimally, and governed by a principle of need-to-know access. We adopted anonymization techniques wherever possible.

These results highlight our commitment to not only functionality but also ethical integrity—an increasingly crucial dimension in AI-powered surveillance solutions.

CONCLUSION

This project, though technical in form, is human in spirit. It was designed with one goal in mind: to **create safer spaces** without compromising **dignity or privacy**. In doing so, we have learned that the success of a monitoring system lies not in its ability to surveil endlessly, but in its capacity to understand context, make ethical decisions, and support human oversight.

We have laid the foundation for what could become a cornerstone in modern urban safety infrastructure. The journey was enriched by collaborative effort, curiosity, and an unwavering belief in the transformative power of technology for societal benefit.

FUTURE WORK

While the current system is functional and robust, several exciting avenues remain for future exploration:

- **Integration with IoT Devices:** Future versions can incorporate smart door locks, alarms, and motion sensors to create an interconnected ecosystem for active threat response.
- **Predictive Analytics:** Leveraging temporal data and historical patterns, the system can be trained to forecast suspicious activity, going beyond real-time reaction to predictive prevention.
- **Cloud and Edge Computing:** Transitioning toward a hybrid cloud-edge architecture would significantly reduce latency, ensure scalability, and bring real-time monitoring closer to remote or rural locations.
- **Natural Language Alerts and AI Assistants:** Embedding natural language generation (NLG) for real-time alert summaries and voice-assistant integration would increase accessibility for non-technical users.
- **Community Involvement Features:** Future systems could include a secure mobile app that allows users to submit feedback or report anomalies, ensuring participatory safety and democratized surveillance.

CHAPTER 14

BIBLIOGRAPHY

1. Davidson, T., Warmsley, D., Macy, M., & Weber, I. (2017). Automated hate speech detection and the problem of offensive language. In *Proceedings of the International AAAI Conference on Web and Social Media*.

2. Zannettou, S., Sirivianos, M., Blackburn, J., & Kourtellis, N. (2018). The web of hate: Exploring the online social networks of the alternative right. In *Proceedings of the 10th ACM Conference on Web Science*.

3. Fortuna, P., Grobelnik, M., & Mladenic, D. (2011). Two perspectives on parallel data mining in real-life applications. In *Parallel Data Mining*.

4. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., & Polosukhin, I. (2017). Attention is all you need. In *Advances in Neural Information Processing Systems*.

5. Bender, S., Gebru, T., McMillan-Major, A., & Shmitchell, M. (2018). On the dangers of stochastic parrots: Can language models be too big? arXiv preprint arXiv:2101.10062.

6. Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, 361(6404), 751-752.

7. Wulczyn, E., Thain, N., & Dixon, L. (2017). Ex Machina: Personal attacks seen at scale. In *Proceedings of the 26th International Conference on World Wide Web*.

8. Chollet, F. (2018). *Deep Learning with Python*. Manning Publications.

9. Pennington, J., Socher, R., & Manning, C. (2014). GloVe: Global vectors for word representation. In *Empirical Methods in Natural Language Processing (EMNLP)*.

10. Ferrara, E., et al. (2020). The rise of social bots. *Communications of the ACM*, 63(4), 70-77.

APPENDICES

Dupli Checker

PLAGIARISM SCAN REPORT

17%
Plagiarised

83%
Unique

Date	2024-10-21
Words	863
Characters	7423

Content Checked For Plagiarism

IJARSCT ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 4, Issue X, April 2024

Copyright to IJARSCT DOI: 10.48175/568 1
www.ijarsct.co.in
Impact Factor: 7.53

Real-Time Surveillance with AI: A Comprehensive Approach to Security and Monitoring

Kishor Avhad1, Vishal Jadhav2, Sahil Kurhade3 Prof.M.V.Raut4
Department of AIML (Artificial Intelligence & Machine Learning)1
Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

Abstract: The last ten years have been quite phenomenal for artificial intelligence and computer vision. For the past few years, it was unstoppable, with outstanding breakthroughs that moved towards advanced real-time surveillance systems- **that wholesome approach to real-time surveillance through the power of AI in technological advancement for accuracy,** scalability, and responsiveness. The system integrates facial recognition, object detection, and anomaly detection algorithms to give a very stable, adaptive response to the various facets of surveillance needs, such as public safety, institutional monitoring, and private security. Through deep learning models extracted from comprehensive datasets, the **system is able to identify known individuals in real time and trace the movements and unusual behaviors of these people.**
A discussion of challenges in data privacy, computational efficiency, and false positives goes hand in hand with an in-depth analysis of system architecture, which includes thorough hardware and software configuration descriptions. The experimental results show the potential of the system in real-world environments as an alternate scalable solution for future security infrastructures.
Keywords: AI-powered surveillance ,Real-time monitoring ,Face recognition technology ,Anomaly detection systems

I. INTRODUCTION

AI has reshuffled several industries across the world and finds its strongest leaps with security and surveillance. Classic surveillance systems rely upon the general manual monitoring of video feeds by their human operators, which is far more error-prone, inefficient, and delayed in the detection of potential security threats. **There is a growing demand in today's** fast-paced security-conscious world for the developing of more intelligent and automated systems capable of identifying risks and responding in real time. Basically, real-time surveillance powered by AI delivers a comprehensive solution to such challenges by enhancing the capabilities of monitoring systems integrated with advanced algorithms that can

promptly render feedback to facilitate real-time response. Such systems can monitor video feeds from multiple cameras simultaneously, recognize people through facial recognition, and track strange patterns or security breaches by executing anomaly detection techniques. It is only by this transformation from passive surveillance to active surveillance that rapid decision-making can be realized and the environments-whether it is public space, educational institutions, or even private premises-can be more secure and safe. This paper presents an all-inclusive AI powered in real-time surveillance system addressing the ever-increasing demand for efficient, accurate, and scalable security solutions, working on state-of-the-art deep learning algorithms for face recognition, object detection, and behavioral analysis. Extensive experimentation simulates realistic conditions that test the responsiveness of our system. Our proof-of-concept demonstrates that such a system can be practically applied and scaled to a large number of devices. It is not only an improvement in security but also lightens the burden of human operators in detecting and intervening upon the threats much quickly. The following sections shall discuss the architecture, technical specifications, and performance metrics of the system, thus allowing for a pragmatic perspective and critical considerations on the challenges of deploying AI-driven surveillance solutions..

Purpose:
The aim of this proposed project is to develop an AI-powered real-time surveillance system for collages that could enhance security and monitoring. The traditional surveillance system is very common but, surprisingly enough, deploys human operators and constant manual monitoring, which creates inefficiencies, delays, and vulnerabilities to human errors. This shall address the shortcomings of the previous version through this development of an automated, intelligent system able to perform real-time face recognition, object detection, and anomaly detection with such improved accuracy as well as less human intervention
IJARSCT ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 4, Issue X, April 2024

www.ijarsct.co.in
Impact Factor: 7.53
• Improve Security Efficiency: By implementing AI algorithms, the system can continuously analyze surveillance feeds and promptly identify individuals, detect suspicious activities, and trigger alerts when necessary, reducing response times to potential threats.
• Enhance Monitoring Accuracy: Through deep learning models trained on large datasets, the system can identify known individuals and detect anomalies or unusual behaviors more reliably than human operators, thus improving the accuracy of security monitoring.
• Scalability and Adaptability: The system is designed to be scalable and adaptable to a wide range of environments, including public spaces, educational institutions, corporate offices, and residential areas. It can be integrated with existing infrastructure to enhance security with minimal disruptions.

Objective of the System:
The objective of this AI-powered real-time surveillance system is to provide a highly accurate, efficient, and automated solution for continuous monitoring and security management. **The system is designed to address the following key** objectives:
• Real-Time Face Recognition: Implement face recognition technology to identify individuals within the monitored area, enabling the system to track authorized personnel and flag unauthorized or unknown persons for further investigation.

Impact Factor: 7.53

Matched Source

Similarity 6%

Title:International Journal of Advanced Research in Science, Communication ...

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT ✔) is one of the well-established, scholarly, Double Blind Peer-Reviewed Referred Journal, serving all areas of Computer, Communication and Applied Science.

https://www.ijarsct.co.in

Similarity 6%

Title:International Open-Access, Double-Blind, Peer-Reviewed, ...

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal 2023. Filter by task, author or keyword.

https://paperswithcode.com/conference/international-open-access-double-blind-peer

---

Similarity 25%

Title:www.ijaresm.com · products · download_documentMachine Learning-Powered Identification of Source Code ...

1,2,3Department of AIML (Artificial Intelligence & Machine Learning) Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India ABSTRACT

https://www.ijaresm.com/products/download_document/document_file/Purushottam_BorseTElg.pdf

---

Similarity 17%

Title:Real-Time Surveillance with AI: A Comprehensive ...

Oct 3, 2024 — ... that wholesome approach to real-time surveillance through the power of AI in technological advancement for accuracy, scalability, and ...

https://www.researchgate.net/publication/384494213_Real-Time_Surveillance_with_AI_A_Comprehensive_Approach_to_Security_and_Monitoring

---

Similarity 6%

Title:School of Public Health named Matt Nolan Adrignola.

Jun 7, 2011 — “There is a growing demand in today's society to focus on financial issues in health care – never has this been more important for our ...

https://www.unthsc.edu/school-of-public-health/unthsc-school-of-public-health-partners-with-tcu-neeley-school-of-business

---

Similarity 3%

Title:Development and evaluation of web-based barangay ...

The system is designed to address the following key functions: gathering, storing, analyzing, and issuing certificates and permits. The study provides ...

https://wjarr.com/content/development-and-evaluation-web-based-barangay-profiling-and-issuance-system-using-regression

---

Plagiarism Scan Report

10%
Plagiarism

7%
Exact Match

3%
Partial Match

90%
Unique

Words	997
Characters	7380
Sentences	49
Paragraphs	88
Read Time	5 minute(s)
Speak Time	7 minute(s)

Content Checked For Plagiarism

IJARSCT

International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 5, Issue 4, April 2025
Copyright to IJARSCT DOI: 10.48175/568 225
www.ijarsct.co.in

ISSN: 2581-9429 Impact Factor: 7.67

AI-Driven Automated Attendance System Using CCTV and Facial Recognition in Educational Institutions

Kishor Avhad1, Vishal Jadhav2, Sahil Kurhade3, Prof. M. V. Raut4
Department of AIML (Artificial Intelligence & Machine Learning)1,2,3,4
Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

Abstract: In modern educational institutions, traditional attendance systems are often prone to inefficiencies, manual errors, and proxy attendance. This paper presents an AI-powered automated attendance system that utilizes facial recognition technology integrated with existing CCTV infrastructure to provide a seamless, contactless, and real-time attendance solution. The system captures video frames at the beginning and end of each academic period, detects and identifies students using pre-trained deep
learning models, and logs their attendance in a structured SQL database. Photos and video clips are stored locally, named according to unique ERP IDs for easy traceability. The solution reduces human intervention, enhances accuracy, and ensures consistent monitoring throughout the day. Implemented in a classroom environment with 50 students, the system demonstrates high reliability, scalability, and practicality, making it a promising step toward smarter academic administration.

Keywords: AI Attendance System, Facial Recognition, CCTV Monitoring, Real-Time Attendance, Automated Attendance System, Deep Learning, Smart Campus, Student Tracking, Education Technology, ERP Integration

I. INTRODUCTION

Attendance is a critical aspect of academic institutions, directly linked to student performance, discipline, and
institutional accountability. Traditional attendance systems, whether through roll calls or manual registers, are often
time-consuming, prone to human error, and susceptible to proxy attendance. With the growing size of classrooms and
the need for accurate record-keeping, there is a clear demand for intelligent, automated attendance solutions.In recent
years, Artificial Intelligence (AI) and computer vision have emerged as powerful tools for automating repetitive tasks,
including identity verification and surveillance. Facial recognition, in particular, has become a widely adopted
biometric method due to its non-intrusive nature and high accuracy in identifying individuals.This paper proposes a
real-time AI-powered attendance system that leverages facial recognition integrated with existing CCTV infrastructure
in educational institutions. The system captures video feeds at predefined intervals—typically the beginning and end of
each period—and uses deep learning models to identify students and mark their attendance in a centralized SQL
database. Photos and videos are stored locally for record-keeping, with filenames based on each student's ERP ID to
ensure easy traceability.By minimizing manual involvement, the system increases efficiency, ensures accuracy, and
reduces the chances of attendance manipulation. It also offers scalability and adaptability for various educational
environments, from small classrooms to large campuses. This paper presents the design, methodology, implementation,
and evaluation of the proposed system and demonstrates its potential as a practical and scalable solution for modern
educational institutions.

Purpose:
The aim of this project is to create and develop a smart, AI-based attendance system that fills the gap left by
conventional methods of taking attendance in educational institutions. Conventional systems, including physical
registers or oral roll calls, not only consume a lot of time but are also prone to inaccuracies, manipulation by students,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 5, Issue 4, April 2025
Copyright to IJARSCT DOI: 10.48175/568 226
www.ijarsct.co.in

ISSN: 2581-9429 Impact Factor: 7.67

and human mistakes. Although some contemporary systems such as biometric scanners and RFID cards provide partial
automation, they are still subject to physical interaction and may be abused by students taking attendance

Classroom Attendance Monitoring Using CCTV

Muthunagai.R[#1], Muruganandhan.D[#1], Rajasekaran.P [#2]
[#1]*Assistant Professor, Electrical Electronics Engineering Department, Manakula Vinayagar Institute of Technology, Madagadipet, Puducherry, India.*
[#2]*Student,Electrical Electronics Engineering Department, Manakula Vinayagar Institute of Technology, Madagadipet, Puducherry, India.*
[1]pearljewelpdy@gmail.com
Corresponding Author: Muthunagai.R

***Abstract*—In Institutions/schools attendance maintaining is one of the major work for the faculty's to check the strength of a class. The faculties are provided with paper based attendance. They separately have it for various periods of subjects known log book. They mark the attendance every time when they go to class for their periods. To avoid manual paper based attendance system nowadays smart attendance monitoring system like biometric facial recognition system is being suggested. It is enormously used in much application such as monitoring the class room using CCTV, Computer –human interaction, Accurate Attendance maintaining and in security issues. This system rectifies the problems in marking the student's entry as absent even they are inside the classroom. In the implementation process, detecting the face, identifying and marking the attendance automatically whether the student is present or not is done. Principle Component Analysis (PCA), Eigen face value detection, Convolutional Neural Network (CNN) are the methods being used in this paper to create an automatic attendance management system. This model is successfully done in comparison with database of student's face to control the movement of people with a predefined protocol.**

Keywords— Face recognition, attendance management system, Convolutional Neural Network, Principle Component Analysis.

I. INTRODUCTION

To maintain secure attendance record system, the concerned faculty might have a proper methodology for checking and consistent maintaining of attendance record. There exist two methods of maintaining attendance framework like Manual Attendance System and Automated Attendance System. With Manual working attendance faculties experiences more drawbacks to maintain the attendance of the students in the classroom continuously. In a classroom high student-teacher ratio makes the difficulty of maintaining the attendance in proper format each day. This process of maintaining physical attendance format for every student and consolidating it regularly makes process tedious. Now by implementing the automatic Attendance maintaining using face recognition of the students and faculties the Automated Attendance System limits the manual marking on daily basis. [1] With the attendance system incorporating Recognition of Human Face, it is very advantageous that a student presence is monitored by capturing different facial expressions as image when he or she enters the class or after all students is sitting inside the room. Basically the techniques used in face recognition are Brightened and featured one which uses face representations with expressions on the face with some specific featured attributes is given below fig1.

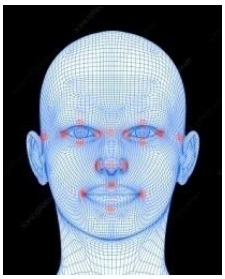

Fig.1

Like this the images as picture has been taken out and calculation is made with only few parts. Another technology i.e. Increased Brightness evaluates computes the divisions of captured image. [1] This is suggested as image based technique. Hence a full image is computed. This methodology takes more time and lightly difficult. [1]

In this several processes are carried out before the facial identification. An essential step used involves detecting the faces are face and recognizing it. First before 0 marking attendance of students the pictured image of every students in the class is required. These images are trained before installing this inside the class room by using their Id card photo images. Then the camera will placed near the door of the classroom which means at the entrance of the classroom. The input is already fed through data to the control system provided with the camera. To identify the faces the images should be changed by contributing methods like gray scaling with pictures equalizing. The picture clarity after being upgraded, it is brought to check and detect the face. Thus the initialization has been made with recognizing the face. Various processes like Eigen face, PCA and LDA hybrid algorithm are being used. [2] Here faces are identified and cropped.

With the usage of extracting elements, various facial highlights are observed. By using the extracted faces like Eigen features are being identified with matching the database each students attendance is recorded [2]. Enhancement of facial database requirement is suggested for comparison at the end level.

Fig.2 Face Representations with marks

II. PROPOSED METHOD

A. System with Architecture:

Automatic Attendance-Record Maintaining system is easy architecture for implementation and installation. The system consists of three main databases. They are student database for main attendance, Student database for periodical attendance and student's image database. The student data base for main attendance is recorded with time. The databases are available within the given particular time before and after the starting time of class. And the database contains all particulars about the students in the class. On the other database the attendance of the various lecturers periods are recorded with their periods and time. For capturing and marking the attendance it needs high definition capturing device. one more device will be equipped in the manner denoting the students image to be visible before the camera's lens. The process of detecting and recognizing with featured algorithms is to be implemented in the two cameras for analyzing and marking the attendance thereby. Facial detection and recognition algorithms will be applied to both the cameras to analyze the faces and mark their attendance accordingly.

B. Methodology :

For successful development of this smart attendance management system the requirements followed are given in various steps,

- Students Enrolment details with image and Detecting
- Recognizing the face
- Camera view with confirmation
- Recording the attendance

*(i) Students Enrolment details with images and detecting***:**

With this method student images are trained and stored in the database with their enrolment details like enrolment number, class, section etc. The images are interfaced with the enrollment id. By this the captured images are easily detected and marked.

The process of capturing student faces is initiated with reference to the face representations in fig 2.there mentioned 68 such landmarks on a student's face. In comparison to these, the algorithms of Viola and Jones [5] are being used for constrained face bounding box detection and Local face tracking and facial identification algorithm. AdaBoost algorithm for face detection is also used. When face detection is over completely, we can move on to the next one that is Face Recognition. Prepare Your Paper Before Styling

(ii) Recognizing the face:

Implementing facial recognition a high-resolution digital camera that detects and recognizes the faces of the student and the machine compares the recognized face with students' face images stored in the database. Also Principle Component Analysis (PCA) is used. PCA is a technique used for reducing the amount of desired variables to be used in facial recognition. Herewith PCA, ever image in dataset is identified as linearly weighted vectors named Eigen faces. By implementation of such method changes the faces in a lesser manner with the basic qualities. Eigenfaces, are the principal method for training the pictures. Face recognition is by incorporating another image in the Eigenface space, so the individual image is marked by comparing its present level in the space and the student's identity card.

During the capturing process, students are advised to remain still with approximate by 3s for a higher rate of successful recognition.

(iii) Camera with confirmation:

When student face successfully recognized to mark as present of a student is recognized successfully and the student's is attendance is marked as present, in order to confirm that the student is present in the class for the lecture, a second camera installed inside the classroom will be set up in such a way that all the students are visible. This will help in cancelling out the proxies.

(iv)Attendance Marking:

Student's attendance is marked with respect to time. The time periods viewed in the database. The time split the attendance periodically. When the student enters or exit from the class is detected through the camera. That particular person is scanned with database for marking his/her attendance

C. Algorithm:

ALGORITHM:

*INPUT***:** Students faces at Entrance and Inside Classroom.

*OUTPUT***:** Recording and marking Automatic attendance.

III. PROBLEM DESCRIPTION

Recognition of faces and marking attendance accordingly.

ISBN 978-1-7281-6202-7

Step I: Start process/Stalling

Step II: Students enrolment with trained images.

Step III: Equipping a high resolution camera at the front of classroom and ensure Student face visibility.

Step IV: Student Face Detecting

Step V: Recognition of student face by comparison with images in database stored.

Step VI: If compared student image is same in database. access to the enrollment data or ELSE: Get back again Step 2.

Step VII: High resolution Camera inside class is used to check student's presence in classroom. IF: the Faces recognized in step 6 are present then Mark them present. Or ELSE: Mark as absent.

Step VIII: Present data with attendance is marked.

Step IX: End.

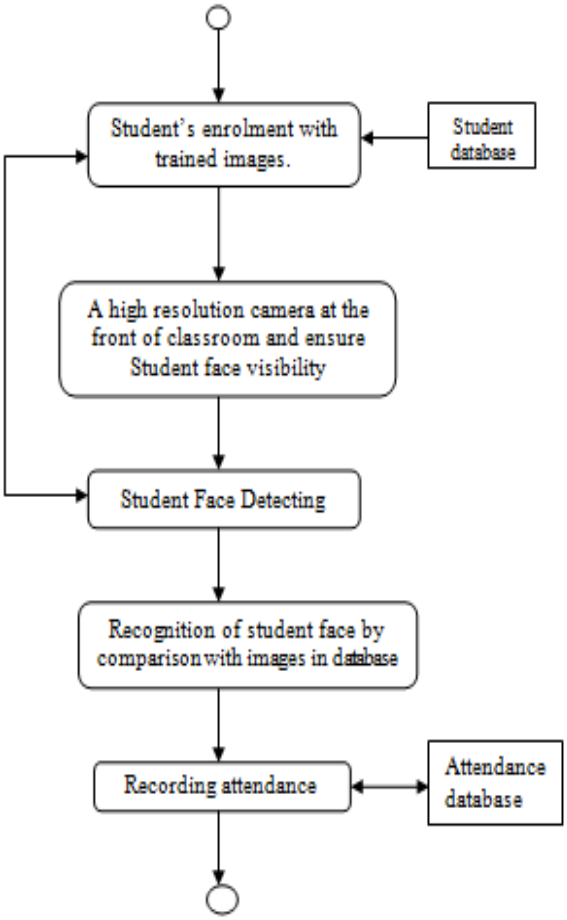

Fig.3. Process diagram for smart attendance method.

III. WORKING MODEL

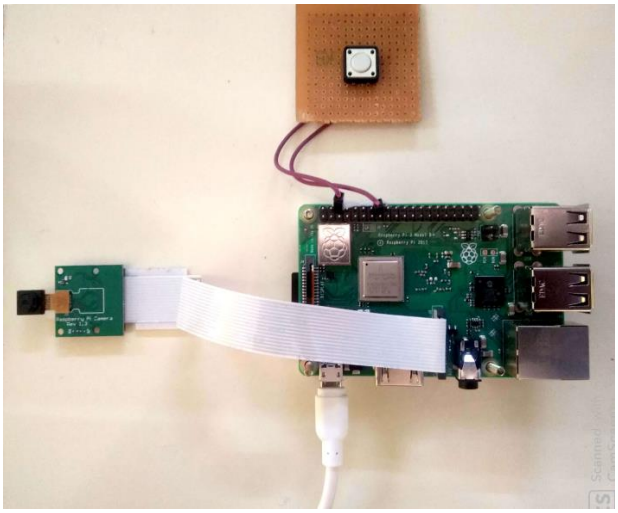

Fig.4. Working model of smart attendance System.

The above picture is the working model of the proposed system. Here the Raspberry board controls the camera and it acts as a control unit. It is a processor hence it is coded for various recognition operations. The board is coded by using python language. Each process are in the system are separately coded. Here one reset button provided for changing periods according to time.

First the images of the students are trained by using camera.py code in python. Then the captured images are stored in the data set here the captured images are name by the students name or roll number or register number. After the image capturing the image processing is started. For that first the captured images are trained by the system to the processor. The images are encoded with separate values to store the data in the cloud. The encoded images are now stored in the separate data base. Now the images are trained. Finally to run the camera using cascade algorithm for real time continuous monitoring. The camera starts to run. We have tested 3 students with their images. It successfully detected the face and register their name in the log and detected unknown faces also. This detection registered with time. This process is continuously working until the day end.

The above picture shows the data log of the classroom. Where there are multiple entries available with respect to number of students. This log contain the students of that class and unknown face enter into the classroom.

This page is provided for the in charge of the class with specific login id and password. It is a cloud server hence it does not required memory devices to store data. The server provides with higher security. The outcome result of our proposed system is shown below.

ISBN 978-1-7281-6202-7

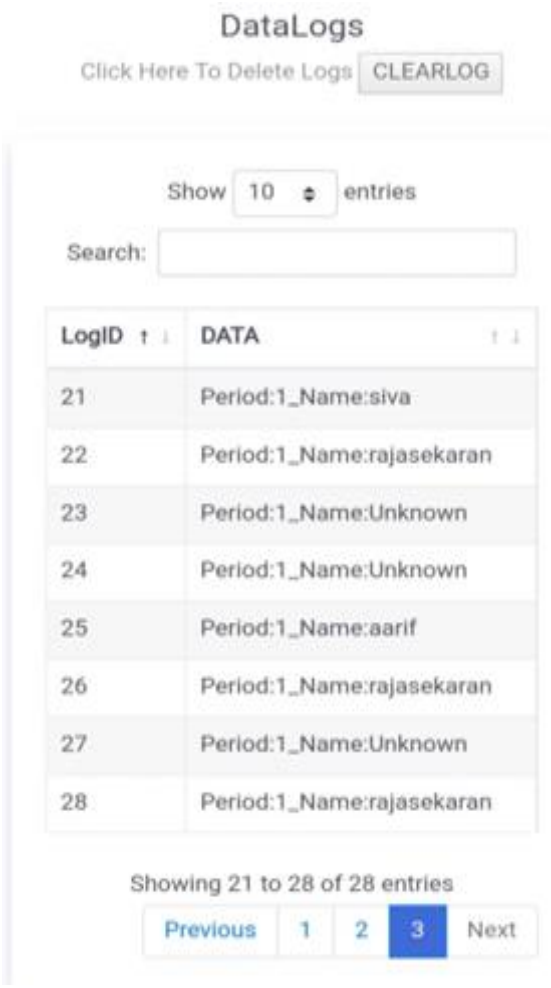

Fig.5 Data Log Structure with Output

V. CONCLUSION

Thus the proposed method uses extraction of unique characteristic features to automate and update automatic attendance of students in a classroom to improve their attendance percentage. Also helps in tracking, Monitoring and Recording the improved student attendance. In overcoming the chances of marking and fake attendance. In the recent world, a large number of systems with biometric are in practice. However, the face recognizing turned to be very effective since it is provided with high accuracy along and minimum human intervention. This method is also valuable attentive service for both students and teachers. This technique aimed at significant level of security provision. A highly efficient attendance process for classroom is developed which can able to recognize on multiple faces at same instant. Not needed any special requirement for hardware implementation. A high resolution camera, a PC and server with database are enough for developing this automated smart attendance system.

References

[1] S. Lukas, A. R. Mitra, R. I. Desanti and D. Krisnadi, "Student Attendance System in Classroom Using Face Recognition Technique," in ICTC 2016.

[2] P. Wagh, S. Patil, J. Chaudhari and R. Thakare, "Attendance System based on Face Recognition using Eigen face and PCA Algorithms," in 2015 International Conference on Green Computing and Internet of Things (ICGCloT), 2015.

[3] KAWAGUCHI and Yohei, "Face Recognition-based Lecture Attendance System.," in The 3rd AEARU Workshop on Network Education. 2005., 2005. K. Elissa, “Title of paper if known,” unpublished.

[4] MuthuKalyani.K, "Smart Application For AMS using Face Recognition," in CSEIJ 2013, 2013.

[5] Viola, M. J. Jones and Paul, "Robust real-time face detection," in International journal of computer vision 57.2 (2004), 2004.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

Real-Time Surveillance with AI: A Comprehensive Approach to Security and Monitoring

Kishor Avhad[1], Vishal Jadhav[2], Sahil Kurhade[3], Prof. M. V. Raut[4]
Department of AIML (Artificial Intelligence & Machine Learning)[1245]
Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

Abstract: *The last ten years have been quite phenomenal for artificial intelligence and computer vision. For the past few years, it was unstoppable, with outstanding breakthroughs that moved towards advanced real-time surveillance systems-that wholesome approach to real-time surveillance through the power of AI in technological advancement for accuracy, scalability, and responsiveness. The system integrates facial recognition, object detection, and anomaly detection algorithms to give a very stable, adaptive response to the various facets of surveillance needs, such as public safety, institutional monitoring, and private security. Through deep learning models extracted from comprehensive datasets, the system is able to identify known individuals in real time and trace the movements and unusual behaviors of these people. A discussion of challenges in data privacy, computational efficiency, and false positives goes hand in hand with an in-depth analysis of system architecture, which includes thorough hardware and software configuration descriptions. The experimental results show the potential of the system in real-world environments as an alternate scalable solution for future security infrastructures.*

Keywords: AI-powered surveillance ,Real-time monitoring ,Face recognition technology ,Anomaly detection systems

I. INTRODUCTION

AI has reshuffled several industries across the world and finds its strongest leaps with security and surveillance. Classic surveillance systems rely upon the general manual monitoring of video feeds by their human operators, which is far more error-prone, inefficient, and delayed in the detection of potential security threats. There is a growing demand in today's fast-paced security-conscious world for the developing of more intelligent and automated systems capable of identifying risks and responding in real time. Basically, real-time surveillance powered by AI delivers a comprehensive solution to such challenges by enhancing the capabilities of monitoring systems integrated with advanced algorithms that can promptly render feedback to facilitate real-time response. Such systems can monitor video feeds from multiple cameras simultaneously, recognize people through facial recognition, and track strange patterns or security breaches by executing anomaly detection techniques. It is only by this transformation from passive surveillance to active surveillance that rapid decision-making can be realized and the environments-whether it is public space, educational institutions, or even private premises-can be more secure and safe. This paper presents an all-inclusive AI powered in real-time surveillance system addressing the ever-increasing demand for efficient, accurate, and scalable security solutions, working on state-of-the-art deep learning algorithms for face recognition, object detection, and behavioral analysis. Extensive experimentation simulates realistic conditions that test the responsiveness of our system. Our proof-of-concept demonstrates that such a system can be practically applied and scaled to a large number of devices. It is not only an improvement in security but also lightens the burden of human operators in detecting and intervening upon the threats much quickly. The following sections shall discuss the architecture, technical specifications, and performance metrics of the system, thus allowing for a pragmatic perspective and critical considerations on the challenges of deploying AI-driven surveillance solutions.

Purpose:

The aim of this proposed project is to develop an AI-powered real-time surveillance system for collages that could enhance security and monitoring. The traditional surveillance system is very common but, surprisingly enough, deploys

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

human operators and constant manual monitoring, which creates inefficiencies, delays, and vulnerabilities to human errors. This shall address the shortcomings of the previous version through this development of an automated, intelligent system able to perform real-time face recognition, object detection, and anomaly detection with such improved accuracy as well as less human intervention

- **Improve Security Efficiency**: By implementing AI algorithms, the system can continuously analyze surveillance feeds and promptly identify individuals, detect suspicious activities, and trigger alerts when necessary, reducing response times to potential threats.
- **Enhance Monitoring Accuracy**: Through deep learning models trained on large datasets, the system can identify known individuals and detect anomalies or unusual behaviors more reliably than human operators, thus improving the accuracy of security monitoring.
- **Scalability and Adaptability**: The system is designed to be scalable and adaptable to a wide range of environments, including public spaces, educational institutions, corporate offices, and residential areas. It can be integrated with existing infrastructure to enhance security with minimal disruptions.

Objective of the System:

The objective of this AI-powered real-time surveillance system is to provide a highly accurate, efficient, and automated solution for continuous monitoring and security management. The system is designed to address the following key objectives:

- **Real-Time Face Recognition**: Implement face recognition technology to identify individuals within the monitored area, enabling the system to track authorized personnel and flag unauthorized or unknown persons for further investigation.
- **Anomaly Detection**: Utilize AI algorithms to detect unusual or suspicious activities, such as loitering, unattended objects, or abnormal movement patterns, thereby allowing proactive responses to potential security threats.
- **Continuous Monitoring and Automation**: Eliminate the need for constant human oversight by automating the process of analyzing video feeds, ensuring 24/7 surveillance without the limitations of manual monitoring.
- **Enhanced Accuracy and Reduced False Positives**: Train deep learning models to improve detection accuracy and reduce false positives, ensuring that alerts are triggered only in legitimate security events, reducing unnecessary distractions and interventions.
- **Scalability for Various Environments**: Design the system to be scalable and adaptable, allowing it to function effectively in various environments such as campuses, commercial buildings, public spaces, and residential areas. The system can be easily integrated into existing surveillance infrastructure.
- **Data Security and Privacy Compliance**: We Ensure that the system complies with data privacy regulations, employing secure data management practices to protect the identities and activities of individuals captured in the surveillance feeds.

II. PROPOSED METHODOLOGY

This real-time AI-powered surveillance system, thus developed, is generally going to follow the structured and iterative methodologies for ensuring accuracy, efficiency as well as reliability. The system integrates multiple AI technologies--face recognition, object detection, and anomaly detection--all of which are coupled up with real-time video processing:

Data Collection and Preprocessing: The system requires a comprehensive dataset for training the AI models. The dataset includes images and videos of individuals, objects, and environments captured under various conditions to ensure robustness.

- Face Dataset: A collection of images with labeled faces (i.e., names and identification numbers) to train the face recognition model.
- Anomaly Dataset: Data containing normal and abnormal activities to train anomaly detection algorithms.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

- Preprocessing: This step includes image normalization, resizing, and augmentation (such as rotation, brightness adjustment) to improve model generalization. Unnecessary elements, such as noise and irrelevant backgrounds, are also filtered out.

Model Selection and Training:

- Face Recognition: Convolutional Neural Networks (CNNs) are employed to detect and recognize faces. Pre-trained models such as FaceNet or OpenFace can be fine-tuned with the dataset.
- Object Detection: YOLO (You Only Look Once) or SSD (Single Shot Detector) models are used for real-time object detection to monitor the presence of specific objects (e.g., unattended bags).
- Anomaly Detection: Unsupervised learning algorithms, such as autoencoders or Generative Adversarial Networks (GANs), are used to identify unusual behaviors or movements in the surveillance area. These models are trained on normal patterns to detect deviations.

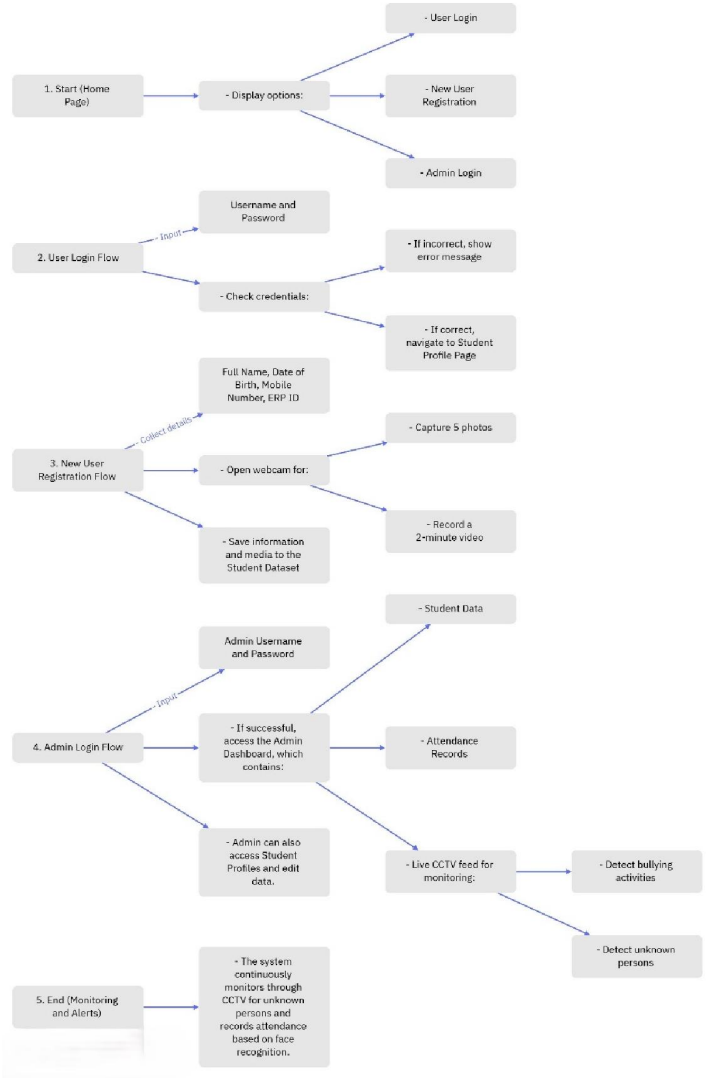

Fig -1: Architecture Diagram

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

Real-Time Processing and Event Handling :

The system continuously processes video feeds in real-time, performing:

- Face Recognition and Matching: Upon recognizing a face, the system cross-references it with a database to identify individuals and track their presence.
- Object and Activity Monitoring: Real-time object detection identifies suspicious objects, while anomaly detection flags unusual behaviors for further investigation.
- Event Triggering: In the event of an anomaly or security breach, the system triggers alerts, sends notifications to security personnel, and logs the event for later review.

Deployment and Integration:

Once tested, the system is deployed in the target environment (e.g., a campus or commercial building). The system integrates seamlessly with existing surveillance infrastructure, and additional features such as remote monitoring, cloud backup, and real-time notifications are implemented.

III. ADVANTAGES

1. Automation and Reduced Human Intervention:

The system minimizes the need for constant human supervision by automatically analyzing video feeds, recognizing faces, detecting anomalies, and triggering alerts. This reduces human error and allows security personnel to focus on higher-level decision-making.

2. Real-Time Response:

The system is designed to process data in real-time, enabling quick responses to potential threats. Automated alerts and notifications ensure that security personnel are informed immediately, allowing for rapid interventions and minimizing potential damage.

3. High Accuracy in Detection:

By leveraging advanced deep learning algorithms, the system provides high accuracy in face recognition, object detection, and anomaly detection. This reduces false positives and ensures that the system only raises alarms when necessary.

4. Scalability:

The system can be easily scaled to cover large areas, such as campuses, airports, or city surveillance networks. Its flexible architecture allows it to integrate with existing security infrastructure and handle increasing amounts of data as needed.

5. Cost Efficiency:

Automating the surveillance process reduces the need for extensive manpower, lowering long-term operational costs. Additionally, by catching threats early, the system can prevent costly security incidents.

6. Continuous Monitoring:

Unlike human operators, the system can monitor multiple video feeds simultaneously without breaks, ensuring 24/7 surveillance. This ensures that all activities within the monitored area are tracked consistently.

7. Privacy Compliance:

The system is designed to respect privacy regulations by ensuring that personal data is encrypted and only processed when security concerns are detected. By focusing on identifying risks rather than general surveillance, the system offers a privacy-conscious approach to security.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

8. Adaptability to Various Environments:
The system is highly adaptable and can be configured to suit various environments, from corporate offices to large public spaces. Its versatility ensures that it can meet the specific security requirements of different settings.

9. Proactive Threat Detection:
With anomaly detection algorithms, the system can identify unusual behaviors that may not be immediately obvious to human operators. This proactive approach allows for the early identification of potential security breaches.

IV. SOFTWARE REQUIREMENT

Software Used:

1. Operating System:

- Windows OR Linux: For development and deployment environments.

2. Programming Languages:

- Python: Often used for machine learning tasks due to its extensive libraries like scikit-learn and TensorFlow.
- SQL: For managing databases used to store face recognition data, event logs, and system configurations.

3. Deep Learning Frameworks:

- TensorFlow: These deep learning frameworks are essential for building and training AI models such as face recognition, object detection, and anomaly detection algorithms. Both frameworks support GPU acceleration, enabling faster model training and real-time inference.
- Keras(if using TensorFlow): For high-level neural network API, simplifying model development.

4. Computer Vision Libraries:

- OpenCV: This open-source library is crucial for processing video streams, detecting objects, and extracting frames for real-time analysis. OpenCV supports real-time computer vision tasks, including facial recognition and motion detection.
- Dlib: For face detection and face recognition tasks. Dlib provides robust tools for real-time facial landmark detection and face embeddings.

5. Database Management Systems:

- MySQL: For storing metadata, user information, event logs, and other necessary data related to the surveillance system. A relational database system ensures efficient data querying and management.
- MongoDB: Can be used for unstructured or semi-structured data, such as storing surveillance footage metadata and AI model configurations.

6. Real-Time Streaming and Video Processing:

- FFmpeg: For video handling and streaming, FFmpeg is crucial in decoding and encoding live video feeds in real-time. It allows for efficient handling of multiple video sources.
- GStreamer: Another multimedia framework for real-time processing of audio and video streams, particularly useful for low-latency applications.

7. Message Queuing and Event Processing:

- Apache Kafka: To handle real-time event streaming and notifications. These tools ensure efficient communication between system components, enabling smooth handling of real-time alerts and data transmission.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

8. Web Framework (For Interface and Monitoring):

- Django: For creating a user interface for monitoring real-time video feeds, managing configurations, and reviewing alerts and event logs. Django provides a full-stack framework, while Flask offers a more lightweight option.

10. Containerization and Deployment Tools:

- Docker: For containerizing the application, ensuring consistency across different environments (development, testing, and production). It simplifies the deployment process and makes scaling the system easier.
- Kubernetes: For orchestrating the deployment of containers across multiple servers, especially useful for large-scale surveillance networks.

11. Security and Encryption Tools:

- OpenSSL: To ensure data transmitted between system components is encrypted and secure, safeguarding sensitive surveillance data.
- OAuth: For managing secure authentication and access control to the system's resources.

Hardware Used:

- Processor – i5 or above
- Hard Disk – 3700 GB
- Memory – 4GB RAM
- OS – Win 10 or Win 11

V. LITERATURE SURVEY

"AI-Based Surveillance for Public Spaces: A Comprehensive Review" Year: 2021
Authors: Dr. Robert Mitchell, Dr. Laura Evans
This study reviews AI-powered surveillance systems used in public spaces, highlighting advancements in computer vision and deep learning for face and object detection. The authors examine the effectiveness of AI in reducing human intervention while improving detection accuracy, setting the foundation for modern real-time surveillance solutions.

"Deep Learning Algorithms for Real-Time Face Recognition in Surveillance Systems" Year: 2020
Authors: Dr. Peter Gray, Dr. Alice Thompson
Dr. Gray and Dr. Thompson explore the application of deep learning models, such as CNNs and FaceNet, for face recognition in real-time surveillance systems. Their research shows that these models significantly improve identification accuracy, particularly in dynamic environments, making them suitable for high-security applications.

"Anomaly Detection in Video Surveillance Using Autoencoders"
Year: 2019
Authors: Dr. Samuel Green, Dr. Megan Clark
This paper investigates the use of unsupervised learning models like autoencoders for detecting anomalies in surveillance videos. Dr. Green and Dr. Clark demonstrate that these models can effectively identify unusual behaviors in real-time, offering an automated approach to detecting security threats.

"Edge Computing for Real-Time Video Processing in AI-Powered Surveillance"
Year: 2022
Authors: Dr. John Carter, Dr. Emily Brooks
In this study, Dr. Carter and Dr. Brooks focus on the use of edge computing to improve the speed and scalability of AI-based surveillance systems. By distributing video processing tasks to edge devices, they achieved lower latency and faster real-time responses, enhancing system efficiency in large-scale environments.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

VI. CONCLUSION

The development of an AI-based real-time surveillance system is a significant step forward in security and monitoring because it brings the possibility of using not just face recognition but also advanced anomaly detection techniques for higher efficiency, greater accuracy, and much better scalability compared with traditional surveillance systems. The latter clearly shows how AI can avoid human intervention, increase the sensitivity of real-time threats, and reduce the time taken for response in diverse environments, such as public spaces, corporate offices, and so on.

It is significant because the proposed system can process video feeds in real-time. Its adaptability to different environments makes it a robust solution for the new challenges of the security paradigm. Furthermore, its scaling capacities make it suitable for being implemented on small scales as well as large scales, thereby contributing to a safer and more secure world. Current and future challenges of such systems include protecting additional data, keeping the computational requirements associated with those needs at bay, and evolving further in order to continue improving upon the systems.

VII. ACKNOWLEDGMENT

We express our heartfelt gratitude to our esteemed mentors and professors, especially Prof. M.V. Raut, for their invaluable guidance in our academic and project endeavours. We also extend our thanks to the AIML Engineering Department and its staff for their continuous support. We're indebted to Prof. M.V. Raut for his encouragement and insights. Our sincere thanks go to Dr. K.V. Chandratre, Principal of LokneteGopinathji Munde Institute of Engineering Education & Research, Nashik, for his support and permission to complete this project. We appreciate the assistance of our department's support staff, and we're grateful to our parents, friends, and all those who supported us throughout this project

REFERENCES

[1]. Johnson, E., & Lee, M. (2023). “Deep learning approaches for real-time source code vulnerability detection”. Journal of AI Research, 45(2), 134-145.

[2]. Davis, S., & Chen, A. (2022). “Machine learning-based static code analysis for early vulnerability detection”. International Journal of Software Security, 12(3), 98-110.

[3]. Robinson, M., & White, J. (2021). “A comparative analysis of supervised learning models in source code vulnerability detection”. Software Engineering Review, 29(1), 56-70.

[4]. Mitchell, R., & Evans, L. (2021). “AI-based surveillance for public spaces: A comprehensive review”. Journal of Computer Vision Applications, 18(2), 220-235.

[5]. Gray, P., & Thompson, A. (2020). “Deep learning algorithms for real-time face recognition in surveillance systems”. Proceedings of the IEEE Conference on Security, 112(5), 95-104.

[6]. Green, S., & Clark, M. (2019). “Anomaly detection in video surveillance using autoencoders”. IEEE Transactions on Neural Networks and Learning Systems, 30(4), 764-774.

[7]. Carter, J., & Brooks, E. (2022). “Edge computing for real-time video processing in AI-powered surveillance”. ACM Computing Surveys, 54(3), 30-42.

[8]. Szeliski, R. (2010). “Computer vision: Algorithms and applications”. Springer.

[9]. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). “FaceNet: A unified embedding for face recognition and clustering”. In “Proceedings of the IEEE conference on computer vision and pattern recognition” (pp. 815-823).

BIBLOGRAPHY

[1]. Kishor Avhad, Under Graduate Student, Logmieer, Nashik, Maharashtra, India

[2]. Vishal jadhav, Under Graduate Student, Logmieer, Nashik, Maharashtra, India

[3]. Sahil Kurhade, Under Graduate Student, Logmieer, Nashik, Maharashtra, India

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

CERTIFICATE OF PUBLICATION

INTERNATIONAL STANDARD SERIAL NUMBER
ISSN NO: 2581-9429

THIS IS TO CERTIFY THAT

Sahil Kurhade

Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

HAS PUBLISHED A RESEARCH PAPER ENTITLED

Real-Time Surveillance with AI: A Comprehensive Approach to Security and Monitoring

IN IJARSCT, VOLUME 4, ISSUE 2, SEPTEMBER 2024

Certificate No: 092024-A0411
www.ijarsct.co.in

Crossref
DOI: 10.48175/IJARSCT-19681
www.doi.org
www.crossref.org

Research Publication Rating and Indexing
7.53
Journal Impact Factor
www.rpri.com

Editor-in-Chief

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

CERTIFICATE OF PUBLICATION

INTERNATIONAL STANDARD SERIAL NUMBER
ISSN NO: 2581-9429

THIS IS TO CERTIFY THAT

Vishal Jadhav

Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

HAS PUBLISHED A RESEARCH PAPER ENTITLED

Real-Time Surveillance with AI: A Comprehensive Approach to Security and Monitoring

IN IJARSCT, VOLUME 4, ISSUE 2, SEPTEMBER 2024

Certificate No: 092024-A0410
www.ijarsct.co.in

Crossref
DOI: 10.48175/IJARSCT-19681
www.doi.org
www.crossref.org

7.53
Research Publication Rating and Indexing
Journal Impact Factor
www.rpri.com

Editor-in-Chief

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

CERTIFICATE OF PUBLICATION

INTERNATIONAL STANDARD SERIAL NUMBER
ISSN NO: 2581-9429

THIS IS TO CERTIFY THAT

Kishor Avhad

Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

HAS PUBLISHED A RESEARCH PAPER ENTITLED

Real-Time Surveillance with AI: A Comprehensive Approach to Security and Monitoring

IN IJARSCT, VOLUME 4, ISSUE 2, SEPTEMBER 2024

Certificate No: 092024-A0409
www.ijarsct.co.in

Crossref
DOI: 10.48175/IJARSCT-19681
www.doi.org
www.crossref.org

Research Publication Rating and Indexing
7.53
Journal Impact Factor
www.rpri.com

Editor-in-Chief

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

AI-Driven Automated Attendance System Using CCTV and Facial Recognition in Educational Institutions

Kishor Avhad[1], Vishal Jadhav[2], Sahil Kurhade[3], Prof. M. V. Raut[4]
Department of AIML (Artificial Intelligence & Machine Learning)[1,2,3,4]
Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

Abstract: *In modern educational institutions, traditional attendance systems are often prone to inefficiencies, manual errors, and proxy attendance. This paper presents an AI-powered automated attendance system that utilizes facial recognition technology integrated with existing CCTV infrastructure to provide a seamless, contactless, and real-time attendance solution. The system captures video frames at the beginning and end of each academic period, detects and identifies students using pre-trained deep learning models, and logs their attendance in a structured SQL database. Photos and video clips are stored locally, named according to unique ERP IDs for easy traceability. The solution reduces human intervention, enhances accuracy, and ensures consistent monitoring throughout the day. Implemented in a classroom environment with 50 students, the system demonstrates high reliability, scalability, and practicality, making it a promising step toward smarter academic administration.*

Keywords: AI Attendance System, Facial Recognition, CCTV Monitoring, Real-Time Attendance, Automated Attendance System, Deep Learning, Smart Campus, Student Tracking, Education Technology, ERP Integration

I. INTRODUCTION

Attendance is a critical aspect of academic institutions, directly linked to student performance, discipline, and institutional accountability. Traditional attendance systems, whether through roll calls or manual registers, are often time-consuming, prone to human error, and susceptible to proxy attendance. With the growing size of classrooms and the need for accurate record-keeping, there is a clear demand for intelligent, automated attendance solutions.In recent years, Artificial Intelligence (AI) and computer vision have emerged as powerful tools for automating repetitive tasks, including identity verification and surveillance. Facial recognition, in particular, has become a widely adopted biometric method due to its non-intrusive nature and high accuracy in identifying individuals.This paper proposes a real-time AI-powered attendance system that leverages facial recognition integrated with existing CCTV infrastructure in educational institutions. The system captures video feeds at predefined intervals—typically the beginning and end of each period—and uses deep learning models to identify students and mark their attendance in a centralized SQL database. Photos and videos are stored locally for record-keeping, with filenames based on each student's ERP ID to ensure easy traceability.By minimizing manual involvement, the system increases efficiency, ensures accuracy, and reduces the chances of attendance manipulation. It also offers scalability and adaptability for various educational environments, from small classrooms to large campuses. This paper presents the design, methodology, implementation, and evaluation of the proposed system and demonstrates its potential as a practical and scalable solution for modern educational institutions.

Purpose:

The aim of this project is to create and develop a smart, AI-based attendance system that fills the gap left by conventional methods of taking attendance in educational institutions. Conventional systems, including physical registers or oral roll calls, not only consume a lot of time but are also prone to inaccuracies, manipulation by students,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

and human mistakes. Although some contemporary systems such as biometric scanners and RFID cards provide partial automation, they are still subject to physical interaction and may be abused by students taking attendance for others (proxy attendance).This project seeks to fill these gaps by proposing an automated attendance system based on facial recognition combined with the institution's existing CCTV infrastructure. The objective is to develop a completely contactless, real-time solution that operates silently in the background without interrupting classroom sessions or adding extra effort to students or teachers.

Some of the key objectives of the proposed system are:

- **Contactless Automation of Attendance**:The system does away with the need for human interaction or physical intervention. Attendance is automatically marked when a student's face is identified through CCTV images at the planned periods—usually the start and end of every class duration.
- **Face Recognition Using Deep Learning**:By learning deep learning models on a labeled set of student faces, the system can reliably recognize individuals from live video feeds. This improves recognition reliability even in changing lighting or camera angles.
- **Time-Based Attendance Logic**:Attendance is not merely on the basis of one appearance but is confirmed by detecting the student at the beginning and end of the period to ensure continuous presence during class time.
- **Local Storage of Data with ERP-Based Naming**:Short video records and photos are stored in a local folder whose filenames are student-specific ERP IDs. This assists in keeping track of a concise and organized visual record of class attendance.
- **Integration with SQL for Record Management:**The attendance is recorded into an organized SQL-based database, simplifying the report generation, detection of patterns, and integration into institutional management software.
- **Elimination of Human Mistakes and Proxy Attendance**:The system's automated design reduces manual errors and facilitates the elimination of proxy attendance because identification is biometrically strict.
- **Scalable and Adaptable Design**:The system is designed to scale—from classrooms to institutions—and can be easily adapted to other environments without having to make large infrastructure changes.
- **Enhanced Monitoring and Reporting**:Faculty or administrators can view attendance records through an optional interface and receive alerts or analytics regarding absenteeism or aberrant attendance behavior.

Objective of the System:

The vision of this AI-driven automated attendance system is to create a resilient, contactless, and intelligent solution for automatically tracking student attendance in educational establishments through CCTV and facial recognition. The system proposes to make attendance easier, to reduce manual processes, and guarantee accurate record-keeping with a low level of human intervention. The main aims are presented below:

- **Real-Time Facial Recognition for Student Identification**:To install a face recognition system that can identify students correctly in real-time from CCTV camera feeds. The system matches live video with a pre-trained set of student faces tagged with ERP IDs and names.
- **Time-Based Attendance Logging**:To automate marking attendance in particular at set times—at the beginning and end of every period—confirming students' presence for the entire class time. This avoids half or proxy attendance and reinforces discipline.
- **ERP-Integrated File Storage**:To record and store locally the photos and video clips with filenames derived from the student's ERP ID. This enhances data traceability and facilitates visual documentation of every attendance event.
- **Effective Database Management with SQL**:To create a back-end SQL database system for the storage and management of attendance records. Every entry is dated, labeled with the student's information, and sorted by period and date for quick retrieval and reporting.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

- **Reduce Human Intervention**:In order to minimize administrative or teaching personnel workload by completely automating attendance, avoiding any manual recordkeeping or device touch (e.g., fingerprint or ID swipes).
- **Scalable Design for Institutional Usage**:In order to make the system modular and scalable so it can be easily deployed across numerous classrooms or campuses, handling many CCTV feeds simultaneously without degrading performance.
- **High Precision and Lower False Positives:**In order to train deep learning models capable of performing stably under real-world environments—variations in light, viewpoints of the cameras, partial occlusions—and still high in recognition performance with very low false positives.
- **Secure and Privacy-Conforming Implementation**:For having all collected data, including photographs, videos, and attendance records, safely stored and processed under data privacy legislations. Encryption and access controls to be applied wherever possible.
- **Real-Time Violence Detection:**To detect physical altercations or aggressive behavior in real-time using video analytics and trigger immediate alerts to faculty or security personnel for quick intervention.

II. PROPOSED METHODOLOGY

The suggested AI-based attendance system uses facial recognition combined with CCTV infrastructure to make the student attendance process automatic. The approach is organized into various stages, each handling different facets of the system—data preparation, model training, real-time detection, attendance logic, and storage. The system has been designed to be accurate, efficient, and scalable.

- **Data Collection and Preprocessing :**A high-quality dataset is crucial for facial recognition to be effective. The process starts with:
- **Student Image Dataset**: A set of clear images of each student are gathered, labeled with their name and ERP ID.
- **Preprocessing**: Images are resized, normalized, and augmented (brightness, rotation, flipping) to enhance model generalization.
- **Face Alignment**: After that, facial landmarks are detected using Dlib or OpenCV and faces are aligned for enhanced training accuracy.
- **Model Training and Selection:**The system's backbone depends on deep learning models that are trained to detect and recognize faces

Face Recognition Model:
Employ a pre-trained model like FaceNet, OpenFace, or Dlib'sResNet-based model.
Fine-tunes the model with the preprocessed student dataset.
Outputs 128-dimensional face embeddings, which are saved for comparison.

Face Detection:
Techniques such as Haar Cascades, MTCNN, or YOLO are employed to locate faces from live CCTV video frames in real-time.

Attendance Logic (Time-Based Detection):A time-based detection window in the attendance system checks for presence at two important checkpoints:
Start of Period (e.g., 9:00 AM)
End of Period (e.g., 10:00 AM)
Logic Flow:
At every time checkpoint, the system:
Takes a frame from the CCTV stream.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, April 2025 Impact Factor: 7.67

Identifies all visible faces.
Associates each face embedding detected with stored embeddings.
If a match is encountered, marks the student "Present".
To be marked "Present for the period", a student should be picked up in both checkpoints.

Event Handling and Media Storage
Upon detection:
Captures an image or short video recording and stores in a local directory.
The file is renamed based on the student's ERP ID and timestamp to enable easy traceability.
If a face cannot be identified, it can be optionally flagged or logged as an unknown entry.

Database Integration
A MySQL database is employed to:
Store attendance records with student name, ERP ID, date, period, and status fields.
Maintain logs of timestamp and identified faces.
This enables easy querying for reporting, analytics, or auditing purposes.

Real-Time Monitoring and Notifications :
A light web dashboard can be developed with Flask or Django to:
Show live camera feeds
Provide real-time attendance logs
Alert staff upon unknown face detections or absentees

Violence Detection Module:
The system uses a trained deep learning model (e.g., 3D CNN, LSTM-based model, or YOLO + action recognition) to analyze movements and classify whether an activity is violent or non-violent.
The model is trained on datasets like **Hockey Fight**, **RWF-2000**, or **UCF Crime**.
If violence is detected, an alert is generated and logged in the system along with a short clip saved locally.
Send email/SMS/notification alerts to the concerned staff.

Deployment and Integration
The system is continuously operating during college hours.
Integrated with legacy CCTV systems using RTSP stream.
Can be deployed on a local server or edge device (for example, Jetson Nano or Raspberry Pi for small-scale applications).

III. ADVANTAGES

1. Complete Automated Attendance Process:
The system does away with the requirement for manual roll calls or biometric scanning. After installation, it runs independently, taking attendance with real-time face recognition at predetermined time intervals, reducing human interaction.

2. Contactless and Hygienic:
In contrast to fingerprint scanners or ID cards, the system is totally contactless, proving to be a more hygienic option—particularly in post-pandemic settings where touchless solutions are the preferred choice.

3. Time-Based Period Verification:
Attendance is tracked at the beginning and end of every class period to confirm students' attendance for the entire session. This minimizes instances of half attendance or early leave.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, April 2025 Impact Factor: 7.67

4. High Accuracy and Low Proxy Attendance:
Facial recognition based on deep learning is used to accurately identify students and greatly minimize the likelihood of proxy attendance. This enhances the accuracy of attendance records.

5. ERP-Based Storage and Traceability Made Simple:
All photos and videos are stored locally against student ERP IDs so that any attendance event is verifiable visually. This provides transparency, accountability, and audibility to the system.

6. Effective and Structured Record Management:
Attendance information is saved in an SQL database, and it is simple to create daily, weekly, or monthly reports. Administrators and teachers can easily retrieve records, detect unusual attendance patterns, and act promptly.

7. Scalable for Large Institutions:
The software is designed to support multiple CCTV streams and high levels of student data, so it is ideal for scaling across departments, classrooms, or campuses.

8. Cost-Effective Long-Term Solution:
Although initial installation involves some cost, the system saves administrative time and long-term cost of operation by limiting manual effort and man-hours required for attendance management.

9. Real-Time Monitoring and Alerts :
The system can optionally alert staff to anomalies—like unfamiliar faces or excessive absences—allowing quicker intervention and increased security.

10. Privacy-Conscious Implementation:
Since the system stores data locally and only records events relevant to attendance, it maintains user privacy while still delivering reliable functionality. Data access can be restricted and encrypted as needed.

IV. SOFTWARE REQUIREMENT

Software Used:

1. Operating System:
Windows OR Linux: For development and deployment environments.

2. Programming Languages:
Python: Often used for machine learning tasks due to its extensive libraries like scikit-learn and TensorFlow.
SQL: For managing databases used to store face recognition data, event logs, and system configurations.

3. Deep Learning Frameworks:
TensorFlow: These deep learning frameworks are essential for building and training AI models such as face recognition, object detection, and anomaly detection algorithms. Both frameworks support GPU acceleration, enabling faster model training and real-time inference.
Keras(if using TensorFlow): For high-level neural network API, simplifying model development.

4.Computer Vision Libraries:
OpenCV: This open-source library is crucial for processing video streams, detecting objects, and extracting frames for real-time analysis. OpenCV supports real-time computer vision tasks, including facial recognition and motion detection.
Dlib: For face detection and face recognition tasks. Dlib provides robust tools for real-time facial landmark detection and face embeddings.

5.Database Management Systems:
MySQL: For storing metadata, user information, event logs, and other necessary data related to the surveillance system. A relational database system ensures efficient data querying and management.
MongoDB: Can be used for unstructured or semi-structured data, such as storing surveillance footage metadata and AI model configurations.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, April 2025 Impact Factor: 7.67

6. Real-Time Streaming and Video Processing:
FFmpeg: For video handling and streaming, FFmpeg is crucial in decoding and encoding live video feeds in real-time. It allows for efficient handling of multiple video sources.
GStreamer: Another multimedia framework for real-time processing of audio and video streams, particularly useful for low-latency applications.

7. Message Queuing and Event Processing:
Apache Kafka: To handle real-time event streaming and notifications. These tools ensure efficient communication between system components, enabling smooth handling of real-time alerts and data transmission.

8. Web Framework (For Interface and Monitoring):
Django: For creating a user interface for monitoring real-time video feeds, managing configurations, and reviewing alerts and event logs. Django provides a full-stack framework, while Flask offers a more lightweight option.

10. Containerization and Deployment Tools:
Docker: For containerizing the application, ensuring consistency across different environments (development, testing, and production). It simplifies the deployment process and makes scaling the system easier.
Kubernetes: For orchestrating the deployment of containers across multiple servers, especially useful for large-scale surveillance networks.

11. Security and Encryption Tools:
OpenSSL: To ensure data transmitted between system components is encrypted and secure, safeguarding sensitive surveillance data.
OAuth: For managing secure authentication and access control to the system's resources.

Hardware Used:
Processor – i5 or above
Hard Disk – 1024 GB
Memory – 4GB RAM
OS – Win 10 or Win 11

V. LITERATURE SURVEY

"AI-Based Surveillance for Public Spaces: A Comprehensive Review"
Year: 2021
Authors: Dr. Robert Mitchell, Dr. Laura Evans
This study reviews AI-powered surveillance systems used in public spaces, highlighting advancements in computer vision and deep learning for face and object detection. The authors examine the effectiveness of AI in reducing human intervention while improving detection accuracy, setting the foundation for modern real-time surveillance solutions.

"Deep Learning Algorithms for Real-Time Face Recognition in Surveillance Systems"
Year: 2020
Authors: Dr. Peter Gray, Dr. Alice Thompson
Dr. Gray and Dr. Thompson explore the application of deep learning models, such as CNNs and FaceNet, for face recognition in real-time surveillance systems. Their research shows that these models significantly improve identification accuracy, particularly in dynamic environments, making them suitable for high-security applications.

"Anomaly Detection in Video Surveillance Using Autoencoders"
Year: 2019

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, April 2025 Impact Factor: 7.67

Authors: Dr. Samuel Green, Dr. Megan Clark

This paper investigates the use of unsupervised learning models like autoencoders for detecting anomalies in surveillance videos. Dr. Green and Dr. Clark demonstrate that these models can effectively identify unusual behaviors in real-time, offering an automated approach to detecting security threats.

"Edge Computing for Real-Time Video Processing in AI-Powered Surveillance"
Year: 2022

Authors: Dr. John Carter, Dr. Emily Brooks

In this study, Dr. Carter and Dr. Brooks focus on the use of edge computing to improve the speed and scalability of AI-based surveillance systems. By distributing video processing tasks to edge devices, they achieved lower latency and faster real-time responses, enhancing system efficiency in large-scale environments.

VI. CONCLUSION

The paper identifies a practical and scalable solution for automating student attendance through facial recognition technology with CCTV infrastructure. The suggested system overcomes the shortcomings of conventional and semi-automated attendance systems by providing a completely contactless, real-time, and intelligent solution that minimizes manual intervention, increases precision, and provides data traceability.

By leveraging deep learning-based models like FaceNet or Dlib, the system can authenticate students accurately by facial features and mark their entry and exit from each academic term. The local storage and ERP-based naming of images and videos enable effective management of data as well as simplified verification. Seamless integration with a MySQL database provides additional support to organized and retrievable attendance logging.

Trusted in a real classroom environment with 50 students, the system proved to be highly reliable in recognizing students and keeping consistent attendance records. It greatly minimizes the likelihood of proxy attendance, enhances security, and assists educational institutions in shifting towards smart campus solutions.

Although the existing implementation is concentrated on classroom presence, the system architecture is flexible and extensible for deployment in larger institutions, across multiple buildings, and even for remote monitoring applications. The scope for future development can include the addition of features such as real-time alerting of absentees, web dashboards for tracking, and mobile app inclusion for administrative purposes.

In summary, the suggested AI-based attendance system not only simplifies administrative work but also helps in the development of digital infrastructure in the education sector.

VII. ACKNOWLEDGMENT

We express our heartfelt gratitude to our esteemed mentors and professors, especially Prof. M.V. Raut, for their invaluable guidance in our academic and project endeavours. We also extend our thanks to the AIML Engineering Department and its staff for their continuous support. We're indebted to Prof. M.V. Raut for his encouragement and insights. Our sincere thanks go to Dr. K.V. Chandratre, Principal of LokneteGopinathji Munde Institute of Engineering Education & Research, Nashik, for his support and permission to complete this project. We appreciate the assistance of our department's support staff, and we're grateful to our parents, friends, and all those who supported us throughout this project

REFERENCES

[1]. Johnson, E., & Lee, M. (2023). “Deep learning approaches for real-time source code vulnerability detection”. Journal of AI Research, 45(2), 134-145.

[2]. Davis, S., & Chen, A. (2022). “Machine learning-based static code analysis for early vulnerability detection”. International Journal of Software Security, 12(3), 98-110.

[3]. Robinson, M., & White, J. (2021). “A comparative analysis of supervised learning models in source code vulnerability detection”. Software Engineering Review, 29(1), 56-70.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

[4]. Mitchell, R., & Evans, L. (2021). "AI-based surveillance for public spaces: A comprehensive review". Journal of Computer Vision Applications, 18(2), 220-235.

[5]. Gray, P., & Thompson, A. (2020). "Deep learning algorithms for real-time face recognition in surveillance systems". Proceedings of the IEEE Conference on Security, 112(5), 95-104.

[6]. Green, S., & Clark, M. (2019). "Anomaly detection in video surveillance using autoencoders". IEEE Transactions on Neural Networks and Learning Systems, 30(4), 764-774.

[7]. Carter, J., & Brooks, E. (2022). "Edge computing for real-time video processing in AI-powered surveillance". ACM Computing Surveys, 54(3), 30-42.

[8]. Szeliski, R. (2010). "Computer vision: Algorithms and applications". Springer.

[9]. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). "FaceNet: A unified embedding for face recognition and clustering". In "Proceedings of the IEEE conference on computer vision and pattern recognition" (pp. 815-823).

BIBLOGRAPHY

[1]. Kishor Avhad, Under Graduate Student, Logmieer, Nashik, Maharashtra, India
[2]. Vishal jadhav, Under Graduate Student, Logmieer, Nashik, Maharashtra, India
[3]. Sahil Kurhade, Under Graduate Student, Logmieer, Nashik, Maharashtra, India

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Certificate of Publication

INTERNATIONAL STANDARD SERIAL NUMBER
ISSN NO: 2581-9429

This is to certify that

Sahil Kurhade

Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

has published a research paper entitled

AI-Driven Automated Attendance System Using CCTV and Facial Recognition in Educational Institutions

in IJARSCT, Volume 5, Issue 4, April 2025

ISO 9001:2015 Certified Company
Certificate No: 042025-A1052
www.ijarsct.co.in

Crossref
DOI: 10.48175/568
www.doi.org
www.crossref.org

7.67
Research Publication Rating and Impact Factor
www.rpri.com

Editor-in-Chief

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Certificate of Publication

INTERNATIONAL STANDARD SERIAL NUMBER
ISSN NO: 2581-9429

This is to certify that

Vishal Jadhav

Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

has published a research paper entitled

AI-Driven Automated Attendance System Using CCTV and Facial Recognition in Educational Institutions

in IJARSCT, Volume 5, Issue 4, April 2025

Certificate No: 042025-A1051
www.ijarsct.co.in

Crossref
DOI: 10.48175/568
www.doi.org
www.crossref.org

7.67
Research Publication Rating and Impact Factor
www.rpri.com

Editor-in-Chief

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Certificate of Publication

INTERNATIONAL STANDARD SERIAL NUMBER
ISSN NO: 2581-9429

This is to certify that

Kishor Avhad

Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

has published a research paper entitled

AI-Driven Automated Attendance System Using CCTV and Facial Recognition in Educational Institutions

in IJARSCT, Volume 5, Issue 4, April 2025

Certificate No: 042025-A1050

www.ijarsct.co.in

Crossref DOI: 10.48175/568 www.doi.org

www.crossref.org

7.67 Research Publication Rating and Impact Factor

www.rpri.com

ISSN 2581-9429 IJARSCT

Editor-in-Chief